VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA NÁRODOHOSPODÁŘSKÁ

Zhodnocení budoucnosti Bitcoinu a jiných kryptoměn

Assesing the Future of Bitcoin and Other Cryptocurrencies

Student: Andrea Myslikovjanová

Vedoucí bakalářské práce: Ing. Emil Adámek

Ostrava 2018

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra národohospodářská

Zadání bakalářské práce

Student: **Andrea Myslikovjanová**

Studijní program: B6202 Hospodářská politika a správa

Studijní obor: 6202R027 Národní hospodářství

Téma: Zhodnocení budoucnosti Bitcoinu a jiných kryptoměn
Assessing the Future of Bitcoin and Other Cryptocurrencies

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Úvod
2. Teoretické aspekty peněz a kryptoměn
3. Analýza kryptoměn
4. Zhodnocení kryptoměn se zaměřením na Bitcoin
5. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků bakalářské práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

JÍLEK, Josef. *Finance v globální ekonomice I. Peníze a platební styk.* Praha: Grada Publishing, 2013. ISBN 978-80-247-3893-2.
MISHKIN, Frederic S. *The Economics of Money, Banking, and Financial Markets.* 10th ed., Harlow: Pearson, 2013. ISBN 978-0-273-76573-8.
REVENDA, Zbyněk a kol. *Peněžní ekonomie a bankovnictví.* 5. vyd. Praha: Management Press, 2012. ISBN 978-80-7261-240-6.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Emil Adámek**

Datum zadání: 24.11.2017
Datum odevzdání: 11.05.2018

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA * OSTRAVA * Ekonomická fakulta 1

Ing. Jiří Balcar, Ph.D.
vedoucí katedry

prof. Dr. Ing. Zdeněk Zmeškal
děkan fakulty

Prohlašuji, že jsem celou práci, včetně všech příloh, vypracovala samostatně.

Ve Frenštátě p. R. dne 27.4.2018 ..... Andrea Jurníková

jméno a příjmení studenta

Poděkování

Tímto bych chtěla poděkovat panu Ing. Emilovi Adámkovi za velkou pomoc, pevné nervy a příjemnou spolupráci při vypracování této bakalářské práce.

Obsah

1 Úvod

Pojem kryptoměna se na trhu vyskytuje již více než deset let. Jedná se o měny, které nejsou fyzicky hmatatelné. Jsou používány pouze v digitální podobě. Stejně jako s tradičními měnami, tak i s kryptoměnami je možné platit řadu aktiv. Navzájem mají spoustu stejných znaků a vlastností, ale i řadu rozdílných atributů, které měnu určitým způsobem zvýhodňují.

Cílem práce je zjistit, zda mohou kryptoměny v čele s Bitcoinem nahradit současný platební systém tradičních měn. Pokud ne, tak může-li v budoucnu tato situace nastat.

K zjištění dané skutečnosti jsou v práci aplikovány základní statistické výpočty polohových, variabilních a závislostních charakteristik. Dále jsou použity různé metody komparace, deskripce, analýzy a syntézy.

První část práce se zabývá základními charakteristikami peněz, jako je historie, funkce, tvorba a zánik. Dále je pozornost věnována tématu centralizace peněz, která odděluje podstatu tradičních peněz od kryptoměn. Následně, na základě tohoto rozporu, jsou objasněny základní znaky kryptoměn. Čtenář je zde seznámen se základními informacemi potřebnými pro pochopení daného tématu.

Následující část je věnována konkrétnějšímu rozboru tří vybraných kryptoměn Bitcoinu, Ethereu a Litecoinu. Tyto měny jsou v době psaní této práce uváděny na trhu jako nejsilnější a nejznámější digitální měny, u kterých je nejpravděpodobnější, že by mohly v budoucnu nahradit platební systém. Většina této části se věnuje Bitcoinu, jeho podrobnému líčení historie a pojmů s ním souvisejících. Mezi tyto pojmy patří peněženka, transakce, technologie blockchain, hash kódy a těžba. Díky nim je zajištěno odlišné fungování Bitcoinu oproti tradičním měnám. Dále jsou v kapitole stručně charakterizovány kryptoměny Ethereum a Litecoin.

Poslední kapitola je věnována srovnání funkcí klasických měn a kryptoměn, ke kterým jsou připojeny statistické výpočty. Na jejich základě je zjišťována shoda vlastností mezi nimi, a možnost určit, zda mohou zkoumané kryptoměny nahradit stávající platební systém. Na závěr kapitoly jsou přidány informace o různých faktorech, které mají nemalý podíl na vývoj budoucnosti.

2 Teoretické aspekty peněz a kryptoměn

Pro pochopení daného tématu o kryptoměnách je nutné vymezit pojem peníze a s nimi spojené vlastnosti. Díky nim tak lze lépe porozumět podobnosti i odlišnosti peněz a kryptoměn. Druhá část kapitoly se věnuje kryptoměnám a jejich základním charakteristikám.

2.1 Tradiční Peníze

Peníze jsou důležitou součástí ekonomického rozvoje všech zemí. Než se však lidstvo dostalo k papírovým penězům, k bezhotovostnímu platebnímu styku či k dnešním elektronickým penězům, musela proběhnout evoluce peněz. Následující podkapitoly tak obsahují definici peněz a jejich historii, funkce peněz a posléze i jejich tvorbu a zánik. Ke kapitole peníze je dále připojena i část o centrální bance, kde je kladen důraz na emisní funkci. Právě tato funkce centrální banky rozděluje řadu ekonomů na zastánce centralizace peněz a odpůrce. Mezi odpůrci tak jsou často lidé, kteří naopak doporučují používat kryptoměny.

2.1.1 Definice peněz

Pojem peníze lze popsat teoretickou i empirickou definicí. Jak uvádí Revenda (2012), za teoretickou definici peněz lze pokládat veškeré aktivum, za něž je možné zaplatit za zboží a služby nebo vyrovnat dluhy. Důležitým rysem peněz je akceptovatelnost všemi subjekty. Aby tato vlastnost fungovala, je nutné, aby subjekty měly důvěru, že se penězi dá platit. V opačném případě by byli lidé nuceni za účelem placení využívat naturální transakce, kde se zboží smění za jiné zboží, nebo přijmout jinou zahraniční měnu. Posledním důležitým aspektem peněz je kupní síla, která určuje, jakou sumu zboží a služeb při daných cenách lze zakoupit.

Druhou definicí peněz podle Revenda (2012) je stránka empirická. V empirické definici nejsou brány v potaz jen mince, bankovky a vklady na běžných účtech, ale mnohem širší okruh. Díky tomu lze sledovat kvantitativní vývoj skupiny peněz. Takový okruh, jenž je sledován, je nazýván měnový agregát. Dělí se na složky, ve kterých se nachází úhrn peněžních prostředků, jenž mají různou míru likvidity. Značí se velkým písmenem M, za kterým je v České republice jedno číslo na stupnici 1, 2, 3. Čím je číslo větší, tím jsou peníze méně likvidní:

$$M1 = \text{oběživo} + \text{vklady na běžných účtech.} \tag{2.1}$$

Pojmem oběživo se rozumí mince a bankovky, které jsou v oběhu, ne tedy jakékoliv rezervy v hotovosti různých bank. Vklady na běžných účtech jsou tvořeny nebankovními subjekty a mohou být v domácí i cizí měně.

$$M2 = M1 + \text{terminované vklady} \quad (2.2)$$

Tento agregát je méně likvidní než M1, jelikož terminované vklady může subjekt z banky vybrat až po určitém dohodnutém termínu. Zpravidla je splatný do 2 let nebo je opatřen výpovědní lhůtou do 3 měsíců. Opět v domácí i cizí měně.

$$M3 = M2 + \text{krátkodobé cenné papíry nebankovních subjektů v domácí měně} + \text{repo operace} \quad (2.3)$$

M3 je agregát, který je nejméně likvidní ze všech tří agregátů. Aby se krátkodobé cenné papíry staly likvidnějšími, je možné je směnit za oběživo či vklad na běžném účtu. Repo operace znamená přijmutí nadbytečné likvidity všech bank Českou národní bankou, která za tuto likviditu poskytne bankám cenné papíry.

$$\text{Měnová báze} = \text{oběživo v držbě nebankovních subjektů a v pokladnách bank} + \text{povinné minimální a dobrovolné rezervy bank na účtech u centrální banky.} \quad (2.4)$$

ČNB (2017) vymezuje peníze čili peněžní agregáty z tří různých pohledů. Prvním vymezením je harmonizovaná definice sektoru **tvorby peněz**, kde velmi likvidní pasiva vydávají subjekty finančním institucím, které jsou rezidenty ČR, ale nejsou měnovou finanční institucí. Druhou harmonizovanou definicí je sektor **držby peněz**, kde patří všichni rezidenti ČR kromě měnových finančních institucí. Patří zde domácnosti, nefinanční podniky, vládní instituce, fondy sociálního zabezpečení a finanční instituce, které nejsou měnové. Poslední určením je **kategorie pasiv** měnových finančních institucí. Tato pasiva se dělí dle likvidnosti a různých specifik finančních systémů. Obdobně jako výše popsané agregáty, se i tyto agregáty dělí dle eurosystému na úzké peníze (M1), střední (M2) a široké (M3).

V tabulce 2.1 je ukázáno, kam každá položka pasiva patří. Z tabulky lze vidět, že do úzkých peněz patří emitované oběživo a jednodenní vklady, a to jsou položky nejvíce likvidní. Do agregátu pak kromě prvních dvou položek patří i vklady se splatností do 2 let a vklady s výpovědní lhůtou do 3 měsíců. Lze je převést na úzké peníze, ale mohou se vyskytnout problémy s převodem. Poslední složkou jsou široké peníze, mezi které patří kromě M1 a M2 akcie a emitované dluhové cenné papíry do 2 let.

Tab. 2. 1 Rozdělení pasiv peněžních agregátů

Pasiva	M1	M2	M3
Emitované oběživo	x	x	x
Jednodenní vklady	x	x	x
Vklady s dohodnutou splatností do 2 let		x	x
Vklady s výpovědní lhůtou do 3 měsíců		x	x
Repo operace			x
Akcie/podílové listy fondů peněžního trhu			x
Emitované dluhové cenné papíry do 2 let			x

Zdroj: ČNB (vlastní úprava), 2017

2.1.2 Historie a vývoj peněz

Aby bylo možné objasnit princip a funkci peněz, je nutné se zaměřit nejprve na samotnou historii peněz a jejich vývoj. Ze začátku, jak uvádí Jílek (2004), neexistovaly peníze, jaké jsou známy dnes. Obchodovalo se či směňovalo mezi lidmi v naturáliích, (barterový obchod). Zprvu se směňoval jeden kus zboží za jiný kus zboží a postupem času vznikaly kvantitativní poměry mezi směňováním. Tento způsob měl určité nedostatky, jelikož člověk A měl zájem o zboží osoby B, která však zároveň měla zájem o zboží osoby C a nikoli osoby A. Takto vzniklý problém se vyřešil vyřazením daného zboží ze spotřeby a místo toho se používalo plnohodnotných mincí nazývaných komoditní peníze. Takto vzniklé komoditní peníze byly plně akceptovány všemi ekonomickými subjekty, a tak bylo umožněno pokračování v oběhu zboží a služeb. V různých státech představovaly komoditní peníze jiný druh předmětu. Kupříkladu obilí, plátno, dobytek. Nakonec se ukázalo, že nejvhodnějšími platidly byly drahé kovy coby zlato nebo stříbro, jelikož jsou dělitelné a následným dělením neztrácejí svou hodnotu, opět se dají slít dohromady, nekazí se. Následně z těchto kovů vznikly mince, které se razily v mincovnách. Tyto mince byly často raženy s podobiznou panovníka dané doby.

Postupem času docházelo k nedostatku drahých kovů a následnému zlehčování mincí. Jak uvádí Revenda (2013), zlehčování probíhalo v podobě redukování množství zlata v minci či záměnou jiného kovu, zmenšováním mince, nebo navýšením nominální hodnoty dané mince, jež byla uznaná vládou.

Podle Mishkin (2013) nastal problém mincí z drahých kovů díky jejich váze a téměř nemožnému přemísťování z jednoho místa země na jiné. Pokud by si tedy někdo chtěl koupit tenkrát dům, množství kovových mincí by neunesl ani za týden. Proto se vývoj peněz posunul

k lehčí variantě, a to k papírovým penězům. Vznikly tak neplnohodnotné peníze. To znamená, že vláda vyhlásí papírové peníze jako zákonné platidlo, které však nemusí být kryté drahými kovy. Důležitým faktorem je, aby lidé věřili těmto penězům, a aby nebylo možné papírové peníze falšovat. Bylo tedy nutné zavést několik ochranných prvků.

Rozvojem ekonomiky dochází k centralizaci emise bankovek. To představuje výsadní právo na tisknutí bankovek pouze jednoho subjektu, zpravidla centrální bankou. Dále podle Revenda (2013) ve 2. polovině 19. století vznikly bezhotovostní peníze, díky častému ukládání peněz na vkladové účty bank formou záznamu na účtu. Takováto nová podoba peněžních prostředků vložená na účtech slouží k záměru:

- spoření peněz a s nimi spjatý výnos z depozitních úrokových sazeb,
- finance, s nimiž může subjekt zaplatit své závazky vůči dalším subjektům.

2.1.3 Funkce peněz

Aby bylo možné pochopit celkovou podstatu peněz a s nimi spojený zánik peněz, je nutné si vymezit základní funkce peněz. Jurečka a kol. (2010) uvádí 3 základní funkce:

- prostředek směny,
- zúčtovací jednotka,
- uchovatel hodnoty.

Prostředek směny je funkce, kdy je zapotřebí důvěra všech ekonomických subjektů v peněžní prostředky, díky nimž probíhá bezproblémové placení a úhrada zboží a služeb. V době, kdy se používaly mince z drahých kovů jakožto plnohodnotné peníze, byla důvěryhodnost založena na obsahu drahého kovu v minci. Postupem času, kdy se platidlem staly i papírové peníze či bankovky, jež nebyly podložené drahými kovy, tzv. neplnohodnotné peníze, byla důvěryhodnost spjata s panovníkem, který vyhlásil platidlo jako zákonné a nezpochybnitelné.

Druhou funkcí, kterou rovněž uvádí i Revenda (2013), je funkce účetní jednotky, která udává cenu každého aktiva, respektive za kolik peněz si ekonomický subjekt může dovolit určité zboží, služby, práci apod. Účetní jednotka také umožňuje vést účetnictví. V neposlední řadě funkce umožnila snížení transakčních nákladů, které byly spojeny s tzv. barterovým obchodem, kde náklady směny jednoho výrobku za jiný chtěný výrobek byly daleko větší.

Poslední funkcí je funkce uchovatele hodnoty. Mishkin (2013) popisuje, že uchovatel hodnoty spočívá v udržení hodnoty kupní síly v průběhu času. Mnoho lidí své peníze ihned

po přijetí nechce utratit a šetří si je doma, nebo na účtu. Uchovatel hodnoty může být i zakoupený dům, pozemky či nějaké šperky, ale lidé často nikde neinvestují z důvodu likvidity. V tomto případě mají peníze hned k dispozici, jelikož jsou samy o sobě prostředkem směny. Pokud by však člověk měl peníze investované v rodinném domě, dal by část peněz makléřovi za zprostředkování koupě, nebo by cenu domu musel snížit, aby měl peníze co nejdříve. Proto si lidé často nechávají peníze u sebe doma, nebo je spoří na vkladových účtech s malým úrokem či na spořicích nebo terminálových účtech, kde ale časový výběr peněz může být omezený.

Další názor má Revenda (2012), který říká, že uchovatel hodnoty peněz je závislý na kupní síle. Pokud by rostla cenová hladina, kupní síla peněz by klesla. Lidé, kteří si nechávají doma neúročené peníze, tak výrazně tratí. Naopak prostředky, které jsou vloženy na účtech, jsou ohodnoceny podle výše reálných úrokových sazeb. Pokud by sazby byly velmi nízké, je výhodnější peníze investovat do hmotných cenností, jako jsou obrazy, pozemky, šperky aj.

2.1.4 Tvorba a zánik peněz

V dnešní době je podle Jílek (2013) vznik peněz spjat s obchodními bankami, které zákazníkovi, jenž má účet u dané obchodní banky, připíšou danou částku na jeho účet. V současné chvíli však nesmí dojít k odečtení částky na jiném účtu, tzn. peníze jsou nově vytvořeny, nejsou z jiného účtu, a proto se jím říká účetní peníze. Záleží pak na klientech, jestli si peníze vyberou v hotovosti, nebo nikoliv. Stejně jak vznikají, tak i peníze zanikají jako účetní položka. Jak tedy přesně vznikají? Obchodní banky vytvoří peníze formou:

- poskytnutí úvěru,
- úročení vkladů, emitovaných dluhových cenných papírů,
- koupí hmotného i nehmotného majetku či nějakých služeb,
- výplatami a odměnami zaměstnancům bank nebo výplatou dividend a tantiém obchodních společností.

Všechny takto vzniklé peníze poskytuje obchodní banka nebankovním jednotkám. Největší objem peněz vzniká při poskytování úvěru.

Peníze zanikají podle Jílek (2013) obráceným způsobem:

- splacením úvěrů i úroků obchodním bankám,
- prodejem služeb a majetku obchodním bankám,
- koupí akcií, tzn. peníze se mění na nepeněžní závazky,

přičemž všechny tyto úkony provádí nebankovní jednotka. Peníze takto vzniklé, či zaniklé můžou být i v jakýchkoliv cizích měnách. Je nutné podotknout, že nikoli jen obchodní banky ale i jiné nebankovní společnosti, jednotky, můžou poskytovat úvěr, vyplácet dividendy apod.

Jinak popisuje vznik bezhotovostních peněz Revenda (2013). Říká, že bezhotovostní peníze může emitovat jak centrální banka, která je tvoří prostřednictvím bezhotovostních rezerv obchodních bank a nákupem cenných papíru a cizí měny, tak obchodní banky, které přijímají prostředky od nebankovních jednotek nebo poskytují úvěr. V dnešní době jsou peníze vytvořené emisí kryty tzv. aktivy emitentů neboli peněžními prostředky, jenž jsou vytvořené centrální bankou, jsou kryty aktivy obchodních bank. Jen velmi malá část je kryta drahými kovy, převážně zlatem. Aktivy emitentů mohou být cenné papíry, devizové rezervy, nebo povinné minimální rezervy.

2.1.5 Centrální banka jako emitent peněz

Další vlastností peněz, jak již bylo řečeno, je centralizace. To znamená, že peníze jsou spravovány jednou autoritou na jednom místě tzv. centrální bankou. Centrální banka podle Revenda (2012) plní tři základní funkce:

- emisní funkce,
- funkce vrcholného subjektu měnové politiky,
- funkce regulace bankovního systému,

kde je pro tuto práci důležitá zejména první funkce. Zde centrální banka vystupuje jako monopol, který jako jediný má právo emitovat hotovostní peníze na daném území. Na českém území obdržela centrální banka monopol na emisi peněz hned na začátku své činnosti. Do doby, než byly bezhotovostní peníze rozšířeny, byl vliv centrální banky na množství peněz v oběhu obrovský. V minulosti existovalo mnoho bank, kterým bylo povoleno emitovat peníze a vzájemně si konkurovat. Ve většině případech konkurování vedlo ke zhoršení situace a byla tak ve většině zemí zavedena jen jedna banka s povolením. Existuje například i společná centrální banka více zemí (Evropská centrální banka).

Dále Revenda (2012) uvádí, že centrální banka svou důvěryhodnost vytváří velmi pracně a dlouze, ale naopak o ni dokáže velmi rychle a jednoduše přijít.

Zastánci centralizace peněz

Jílek (2004) zastává názor, že centrální banka nikdy nebyla monopolem na emisi peněz, ale na emisi oběživa. Udává, že centrální banka emituje nové peníze pouze při úvěrování klientů, kde funguje jako obchodní banka. Když centrální banka nakupuje či prodává cizí měnu obchodním bankám, nevytváří oběživo, ani nedává důvod k zanikání peněz. Pokud centrální banka emituje hotovostní peníze, není to založené na jejím uvážení, ale na obchodních bankách. Jestliže banky očekávají větší poptávku po hotovosti, koupí si je za peněžní prostředky, které mají u centrální banky uschované na běžném účtu. Centrální banka tak neovlivňuje množství emitovaného oběživa. Je důležité podotknout, že obchodní banky se snaží mít co nejméně peněz v hotovosti, jelikož se tato aktiva nedají úročit.

V jiném svém díle Jílek (2013) uvádí, že příčinou inflace je růst peněžní zásoby, kterou však netvoří centrální banka, ale podniky nebo domácnosti, které si půjčily bankovní úvěr, viz kapitola 2.1.4. Ceny nemovitostí jsou takto nejvíce ovlivňovány objemem hypotečních úvěrů.

Odpůrci centralizace peněz

Podle Rothbard (2001), představitele rakouské školy, jsou zásahy státu a samotná centralizace peněz špatná. Tvrdí, že pokud by vláda chtěla více majetku od ekonomických subjektů, aniž by to byl zločin, stačí jí, aby zavedla daně. Rafinovanější způsob vytvoření peněz, kdy lze vytvořit peníze z ničeho, je nazýván inflací (pokles hodnoty peněz). Zvyšování inflace může vzniknout více způsoby, mezi kterými však dominuje způsob tisknutí peněz monopolní mincovnou, to jest centrální bankou. Následně narůstá pomyslný blahobyt lidí. Pokud jsou tedy centrální bankou natisklé nové peníze a jsou puštěné do oběhu, lidé, jež se dostali k novým penězům jako první, obdrží zisku nejvíce. Avšak lidé, kteří nakupují zdražené zboží dřív, než se jim zvýší plat, naopak tratí. Nejvíce tak trpí zaměstnanci s pevnými mzdami nebo lidé se starobním či invalidním důchodem. Efektivita trhu je tak narušena a všechny podniky jsou najednou prosperující, jelikož vydělávají více peněz. Lidé přestávají spořit, neboť je to poškozuje a začínají si půjčovat. Extrémně tato situace vede k hyperinflaci. Ze začátku, díky vyšším cenám, zůstávají zboží a služby ležet ladem, kvůli vidině lidí, že zboží jistě v budoucnu opět zlevní. Pokud takováto situace nenastane, zboží je naopak kupováno ze strachu dražšího zítřka a ztráty hodnoty peněz. Centrální banka tak podporuje nedostatek peněz dalším tisknutím peněz a dochází tak k čím dál větší inflaci, hyperinflaci.

Zastánci rakouské školy tak kritizuji peníze v rukou státu, který je poškozuje, a naopak zastávají názor decentralizované měny. Není tohle nakonec základní princip kryptoměn?

2.2 Kryptoměny

Následující podkapitoly obsahují teorii o kryptoměnách, jako je základní charakteristika s důležitými vlastnostmi, historie a vznik kryptoměn a následně jsou popsány některé známé druhy kryptoměn.

2.2.1 Charakteristika kryptoměn a jejich klady

Kryptoměna je druh digitální měny, který je šifrován kryptografickým protokolem. Všechny kryptoměny vlastní svou platební síť, ve které je možné provádět transakce. Podle Investplus (2017), jsou platební sítě vytvářeny uživateli, kteří jsou na rovnocenné pozici a pomáhají jednotlivé sítě spojovat a propojovat. Takovým sítím se říká P2P sítě. Jak uvádí Martucci (2017), složité kódování napomáhá přenosu a výměně citlivých dat. Tyto protokoly jsou vytvářeny na základě pokročilé matematiky a počítačového inženýrství. Díky složitosti těchto protokolů je téměř nemožné je padělat nebo je duplikovat (dvakrát tím samým zaplatit něco jiného). Na rozdíl od peněz běžně užívaných a emitovaných centrální bankou a také na rozdíl od jednoduchých digitálních měn, jsou kryptoměny vyznačovány principy, ve kterých jsou odlišné:

- anonymita,
- decentralizace,
- omezené množství,
- transparentnost.

Kryptoměny jsou anonymní. To znamená, že zakrývají identitu uživatele, který měnu používá nebo s ní zrovna platí. Adresa uživatele se skládá pouze z náhodných písmen a číslic, neobsahuje žádné jméno ani bydliště. Finanční toky je následně těžké přiřadit od koho a ke komu putovaly.

Dále jsou kryptoměny decentralizované. Znamená to, že kryptoměnu nikdo nekontroluje, nereguluje ani ji nikdo konkrétní neemituje. Celková hodnota a množství kryptoměn je kontrolována uživateli, jejich aktivitami a zašifrovanými protokoly. Aktivitami uživatelů se myslí tzv. těžení, kde se uživatelé vyskytují pod pojmem těžaři a pomocí těžkých výpočetních technik zaznamenávají transakce a přidávají je za finanční odměnu do řetězce. Těžaři tak zajišťují plynulost a funkci transakcí, viz dále kapitola o těžení. Výhoda decentralizace tak spočívá v tom, že pokud neexistuje hlavní počítač, který by celou kryptoměnu řídil, nemůže se tak hackováním, nebo jiným pirátstvím zničit systém kryptoměn.

Následujícím znakem kryptoměn je konečná nabídka peněz. Díly protokolům je určeno, kolik jednotek měny lze vytěžit. Díky této vlastnosti se tak nemůže stát, že by rostla inflace, naopak je to měna deflační. Často jsou kryptoměny připodobňované ke zlatu, kterého je rovněž omezené množství.

Transparentnost se vyznačuje tím, že každá transakce, jež je provedena, je zaznamenána v digitální účetní knize. Této knize se říká blockchain. Není zde napsáno jméno uživatele, ale pouze kód digitální peněženky, kterou vlastní každý člověk, který chce kryptoměnu vlastnit. Blockchain je volně dostupný a může se na něj kdokoliv kdykoliv podívat. Kryptoměny mají i řadu nevýhod, jako jsou rizika odcizení, nízká likvidita, nebo velká volatilita hodnoty. Kromě toho můžou kryptoměny podporovat kvůli své anonymitě řadu obchodů na černém trhu, proto řada států nedůvěřuje těmto měnám.

2.2.2 Historie vzniku kryptoměn

Podle Csepcsar (2017) byla hlavním popudem pro vznik kryptoměn světová ekonomická krize v roce 2009. Velké firmy a korporace investovaly za vidinou zisku do stále riskantnějších investic, které v případě neúspěchu zachrání stát. Pokud by stát velké firmy nezachraňoval, mohlo by to mít obrovské následky pro ekonomiku. Stát tak měl silnou centralizovanou moc, která se nelíbila mnoho odpůrcům. Vznikly tak decentralizované systémy kryptoměn, které jsou mimo působnost bank, států a nadnárodních korporací. V roce 2008 vznikla internetová stránka Bitcoin.org, kde byl sdílen dokument Satashi Nakamotem, který objasňuje princip fungování jedné z prvních kryptoměn Bitcoin a stál se tak základem pro všechny ostatní kryptoměny.

První myšlenky kryptoměn jsou zasazeny do 80. let 20. století. Americký kryptograf David Chaum vymyslel algoritmus, který se používá pro šifrování na internetu. Informace jsou díky algoritmu přes internet přenášeny bezpečně a nezaměnitelně. Zásluhou tohoto objevu vznikl základ pro budoucí vznik elektronických peněz. Jak uvádí Martucci (2017), David Chaum chtěl svůj přínos šifrovacího algoritmu zužitkovat, a proto odjel do Nizozemska, kde založil společnost DigiCash. Společnost byla zpočátku úspěšná a vytvářela své měnové jednotky. Firmě ale chyběla důležitá vlastnost decentralizace. Měla monopol na kontrolu nabídky této měny, což negativně ovlivňovalo tržní potenciál. Později bylo firmě zakázáno centrální bankou Nizozemska jednat s jednotlivci. Mohli pouze obchodovat s licencovanými bankami, což měně velmi uškodilo. Firma následně skončila. V podobnou dobu Wei Dai, softwarový inženýr, publikoval knihu o virtuální měnové architektuře, která obsahovala řadu

základních složek, které jsou používány v dnešních kryptoměnách, kupříkladu anonymita a decentralizace. Dalším běžným rysem kryptoměn je použití řetězového bloku, již známý v této práci jako blockchain. Právě tuto technologii vymyslel Nick Szabo, spolupracovník Davida Chauma, který ji aplikoval na své kryptoměně Bit Gold. Tato měna nebyla dostatečně populární a již jako měna nefunguje.

Po ukončení činnosti firmy DigiCash se investice a výzkumy přenesly do jiné oblasti a začal se rozvíjet Paypal. Tento internetový platební systém není anonymní, ale je identifikovaný e-mailovou adresou uživatele. Navíc je propojen s platebními kartami, z nichž se přeposílají na účet Paypal. Výhodou je, že příjemce nezíská přístup k platební kartě odesílatele, nevýhodou však jsou vysoké poplatky transakce (Banky, 2017).

Dalším posunem digitálních měn byla měna e-gold používaná ve Spojených státech. Jak uvádí Martucci (2017), měna fungovala na principu kupování digitálního zlata společnosti, která e-gold vynalezla. Uživatelé posílali své zlaté šperky, mince a jiné do skladu e-goldu a dostávali za ně digitální e-gold měnu. Měna šla pak volně mezi uživateli směnit za zlato nebo za americké dolary. Kvůli špatné bezpečnosti protokolů, které měly digitální měnu chránit před útoky hackerů, měna brzo skončila.

První veřejně používanou kryptoměnou se v roce 2009 stal Bitcoin. Byl založen na pricipu decentralizace, anonymity a používání blockchainu. Po vydání dokumentu člověkem, nebo skupinou nazývanou Satoshi Nakamoto (dodnes se neví, kdo to je), se začala měna vyměňovat a dolovat. Vznikaly burzy Bitcoin a začala vznikat i další významná kryptoměna jako je Litecoin. Bitcoin je však dodnes považován za nejpopulárnější měnu a stále více obchodníků platbu v Bitcoinu přijímá.

2.2.3 Rizika a hrozby kryptoměn

Velkým rizikem kryptoměn podle Investplus (2017), je vysoká volatilita, tudíž velmi nestabilní hodnota kryptoměn. Během jednoho dne může hodnota jednotky kryptoměny spadnou či vzrůst o víc než 1000$. Další hrozbou jsou útoky hackerů, kteří dokážou odcizit kryptoměny nejedné burzy. V dřívějších dobách byly některé kryptoměny dokonce považovány za měnu, kterou používali drogoví dealeři a jiní zločinci. Velký negativní vliv na kryptoměny může mít i prohlášení vlády a kontrolních orgánů, kteří tuto měnu označí jako nelegální, nebo trh kryptoměn výrazně omezí. Za další negativum se považuje vysoká energetická náročnost, kterou těžaři, jenž měnu těží, musí zaplatit.

3 Analýza kryptoměn

V následující kapitole si přiblížíme tři nejznámější kryptoměny, se kterými se dnes dá platit v mnoha obchodech. Každá z nich má podobné vlastnosti a zároveň jiné výhody. Hlavním rozdílem Litecoinu od Bitcoinu jsou rychlejší a levnější transakce, oproti tomu Ethereum obsahuje navíc funkci chytrého kontraktování. Abychom dokázali pochopit podstatu každé z nich, je třeba analyzovat jednotlivé kryptoměny a objasnit si, jak fungují.

3.1 Bitcoin

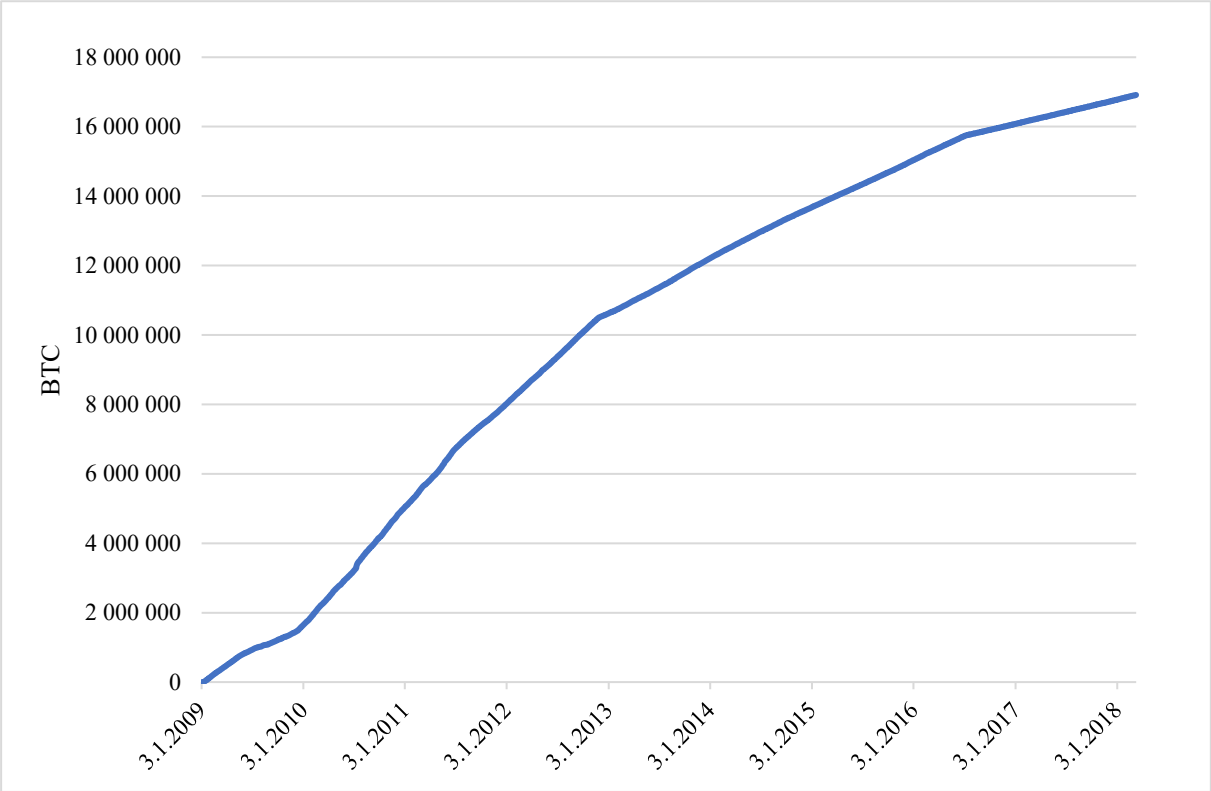
Je jednou z neznámějších a nejstarších kryptoměn. Má vlastnosti klasické kryptoměny, je decentralizovaná a tvořena P2P sítí.

Bitcoin je třeba v rámci práce rozdělit na dva pojmy. Stejně jako uvádí Coindesk (2018), je kryptoměna členěna na bitcoin s malým b a velkým B na začátku slova. Je-li v textu použit pojem bitcoin, jedná se o konkrétní vyjádření jednotky hodnoty, jenž přijímáme nebo posíláme. Zkráceně lze psát jako BTC. Pokud je v textu psán Bitcoin s velkým B, myslí se tím celková distribuovaná síť nebo systém, ve kterém je obchodováno, nebo investováno s bitcoiny. Díky tomuto elektronickému systému je umožněno platit bitcoiny mezi uživateli bez nápomoci třetí strany, tj. platební brány nebo banky. Samotné bitcoiny neexistují v tištěné fyzické podobě (vyjma papírové peněženky, viz kapitola 3.1.2), ale pouze jako elektronické peníze, které jsou produkovány softwary BitTorrent na počítačích uživatelů po celém světě. Bitcoin má vlastnosti společné s tradiční kryptoměnou. Je to například ochota obou stran platit a přijímat peníze elektronicky, stejně jako placení dolary přes účet. Naopak Bitcoin využívá vlastností, které jej od tradičních měn odlišují.

První vlastností je decentralizace. Jak už bylo řečeno, Bitcoin ke svému fungování nepotřebuje žádnou třetí stranu. Je spravován dobrovolnými uživateli, kteří za to dostávají odměnu ve formě bitcoinů. Provozován je veřejnou sítí veškerých uživatelů na celém světě. Uživatelé tak oceňují tento systém díky snižování nepohodlnosti, kterou pociťují u tradičních měn, jež jsou kontrolovány bankami či vládními institucemi. Zároveň systém sám umí skrz kryptografii, kterou používají uživatelé u těžení, eliminovat problémy dvojího utrácení stejných peněz, kterou v případě tradičních měn provádí banky. Druhým znakem Bitcoinu je omezená nabídka. Fiat měny (=tradiční měny) jsou známé neomezeným množstvím nabídky peněz, která je určena centrálními bankami. Centrální banky ovlivňují množství peněz v oběhu, a to často vede k manipulaci hodnoty měny, tzv. inflaci. Oproti tomu je Bitcoin řízen

algoritmem, který určuje, kolik nových bitcoinů je možné za každou hodinu vytěžit. Tohle množství se díky algoritmu co čtyři roky snižuje na polovinu, dokud nebude vytěženo 21 milionů BTC. Obrázek 3.1. ukazuje na celkové množství bitcoinů, které již byly vytěženo. Od ledna 2018 dosáhl Bitcoin 80 % vytěženého množství. Pokud by poptávka po kryptoměně rostla, hodnota jednoho BTC by se zvyšovala díky jinak stejné nabídce.

Obr. 3. 1 Celkové množství vytěženého BTC v čase (2009-2018)



Zdroj: Blochchain (2018), vlastní úprava

Třetím atributem je pseudonymita neboli anonymita. Na rozdíl od tradičních měn, kde se člověk při placení musí identifikovat (kvůli ověření různých předpisů), je Bitcoin založen na poloanonymitě. Není zde třetí strana, která by identifikaci kontrolovala, ale i tak zde určité ověření funguje. Pokud je uživatelem odeslána transakce, protokol, na kterém Bitcoin funguje, prověří veškeré transakce, které proběhly dříve a potvrdí, zda bitcoiny jsou skutečně vlastněny odesílatelem a zda je možné je odeslat. K tomuto úkonu není potřeba znát identitu uživatele. Avšak i když není uživatel identifikován jménem, bydlištěm nebo číslem občanky, je určen adresou své peněženky. Lze proto sledovat určitou adresu a její transakce. Nadto hodně serverů, přes které lze nakupovat či prodávat bitcoiny, požadují při první registraci zákazníka identifikaci totožnosti. Díky tomu, že je síť transparentní, je možné veškeré platby najít jakýmkoliv uživatelem. Proto se uvádí, že Bitcoin není optimální pro teroristy, zločince

nebo jiné uživatele, kteří by zde chtěli špinavé peníze prát. Další výhodou či nevýhodou je změnitelnost. Pokud jsou bitcoiny odeslány, není zde možnost množství upravit či vrátit zpátky. Je to dáno neexistencí centrální autority, která by rozhodla o právu peníze vrátit. Za klad nezměnitelnosti by bylo možné označit fakt, že žádná platba v rámci sítě Bitcoin nelze zmanipulovat. Poslední vlastností, kterou server Coindesk (2018) uvádí, je dělitelnost. Jeden bitcoin lze dělit na spoustu menších částí, kdy v dnešní době je nejmenší část nazývána satoshi. Jeden satoshi se rovná 0,00000001 BTC. Tato vlastnost umožňuje provádět mikrotransakce, které v případně tradiční měny nejsou zcela možné.

3.1.1 Vznik Bitcoinu

Konkrétní vznik Bitcoinu se datuje od roku 2009, kdy byl vývojářem člověk, nebo skupina lidí, kteří se kryjí pod přezdívkou Satoshi Nakamoto. Zanedlouho po vypuštění kryptoměny do světa dal Satoshi svou doménu Bitcoin.org příznivci Gavinovi Andersonovi a přestal jakkoliv spolupracovat. Od té doby je neznámý a lidé hledají jeho identitu. Podle Stroukal (2015), se nejednalo o Japonce, ale o anglicky mluvícího člověka, jelikož psal výbornou angličtinou s britským nářečím. Je možné, že Satoshim bylo více lidé, kteří bylo výborní v ekonomice, informatice i kryptografii. Další možností, kdo by mohl být Nakamoto, byl irský student Michael Clear. Uměl ekonomii, na škole byl nejlepším žákem kryptografie a zaměstnávala ho irská banka, kde pro ni zkvalitňoval software ohledně obchodu s měnami. Michael však popřel, že by měl cokoliv s kryptoměnou společného.

Kollarčík (2017) píše, že by pseudonymem Nakamoto mohla označovat skupina tří osob, a to Neala Kinga, Vladimira Oksmana a Charlese Bry. Pravý Nakamoto totiž napsal studii o Bitcoinu a jeden novinář napsal části této studie do Google vyhledávače a našel tak velkou podobu textu s patentem těchto tří lidí. Zajímavé je, že patent, který byl o šifrování klíčů, byl podán jenom o tři dny dříve, než byla registrována samotná doména Bitcoin.org. Avšak i tato téze byla autory patentu popřena. Dále autor uvádí za možného tvůrce kryptoměny Jeda McCaleba, který žil v Japonsku a vytvořil směnárnu Mt. Gox a jiné decentralizované platební systémy.

Největším podezřelým podle Stroukal (2015) od března 2014 byl Japonec, který žil v Americe, Dorian Nakamoto. Narozený jako Satoshi. Pracoval pro finanční instituce a sám policii tvrdil, že už se tomu nevěnuje a přenechal to ostatním. Avšak Dorian posléze několikrát novinářům odpověděl, že nic o Bitcoinu neví a že policií odpovídal pouze na smlouvu, co kdysi měl s armádou Spojených států. Skutečný Satoshi se však po tak dlouhé době ozval a na svém

profilu napsal, že není Dorianem. Od té doby už se neozval. Zřejmě nejblíže k Satoshimu má programátor z Ameriky Nich Szabo. Nick napsal článek o bit gold, kde často používal jeho pseudonym a tvrdil, že jenom on se svými přáteli uvažovali nad Bitcoinem dřív, než Nakamoto vydal svou doménu. Pozoruhodná je i shoda písmen na začátku jmen obou mužů.

Coindesk (2016) uvádí, že od prosince 2015 je známá další identita Nakamota v souvislosti s australským podnikatelem Craig. S. Wright. Ten identitu nepopřel. Důkazů však není dostatečné množství.

Původce Bitcoinu není tak důležitý jako to, že vznikla měna, která funguje a která nepotřebuje žádného vůdce.

3.1.2 Peněženka

Aby bylo možné bitcoiny používat, je třeba si nejprve pořídit bitcoinovou peněženku. Zdánlivě může připomínat peněženku, která se používá v každodenním životě při placení s hotovostními penězi či penězi na kartě. Rozdílem je, že ve většině případů nenabývá materiální podoby, ale je digitální. Je možné mít peněženku na počítači nebo na chytrém mobilním telefonu s androidem nebo na fyzickém úložném prostoru či na papíře. Záleží pouze na uživateli, jakou metodu si vybere a jaké značce bude věřit. Podle Bešťák (2014), lze z každé peněženky přijmout nebo poslat bitcoiny na jakoukoliv adresu. Pokud uživatel chce příjmout bitcoiny jiného uživatele, musí mu sdělit svou adresu, kterou mu vygeneruje jeho peněženka a poslat ji druhému uživateli. Takováto adresa se skládá z písmen a číslic, které představují veřejný klíč, zmenšený na tzv. hash. Pro ukázku vypadá například takto: 1MdSPSXmT4yGQ9vTsbiZT4BqZfYMC1L7T7. Kromě veřejného klíče peněženka vygeneruje i klíč soukromý, který zůstává bezpečně uschovaný před ostatními držiteli bitcoinu. Pro přijmutí bitcoinu je tedy nutné sdělit veřejný klíč odesílateli a zároveň znát svůj soukromý klíč pro podepsání transakce. Bez privátního klíče nelze poznat, které transakce patří dané peněžence. Aby bylo užívání jednodušší, byly vymyšlené peněženky, které jedním kliknutím bitcoiny odesílají i přijímají.

Druhy peněženek jsou rozlišovány zejména na ty, jež jsou připojeny k síti, jsou jednodušší na ovládání, přijatelnější, ale méně bezpečné. A na ty, které nejsou připojené a jsou bezpečnější. A to z důvodu neopouštění soukromého klíče ze zařízení a nemožnosti útočníku se dostat do zařízení přes síť. Nevýhodou je pomalejší rychlost.

Druhy peněženek:

- softwarové,
- online,
- mobilní,
- hardwarové,
- papírové.

První a častou možností je softwarová peněženka. Podle Marty (2017) to znamená, že je uložena na počítači uživatele bitcoinu, který si stáhl některého z klientů. Buď je stažen plnohodnotný klient (tlustý klient), který je nejbezpečnější volbou a původním originálem, avšak zabírá spoustu místa v řádu stovek GB kvůli stahování celého blockchainu. Nebo je stažena odlehčená verze tzv. tenký klient. Výhodou je, že nezabírá mnoho místa, ale díky absenci blochchainu může transakce trvat několik sekund až minut. Základem bezpečnosti je zvolení dobrého složitého hesla. Většinou jsou softwarové peněženky lehké na ovládání a jsou zadarmo. Nevýhodou může být odcizení počítače, kde může zloděj najít peněženku i s nechráněnými soukromými klíči, a tak všechny bitcoiny ukrást.

Online peněženky jsou podle Tradearena (2018) nejjednodušším řešením. Avšak už z názvu je jasné, že jde o peněženku, která je připojena k síti, a proto není příliš bezpečná. Jsou uložené na cizích serverech a také jim chybí důležitá funkce tzv. anonymita. Je to dané tím, že při registraci na online stránku vyžadují burzy znát údaje o osobě, která se rozhodla online peněženku používat. Nejznámější internetovou stránkou pro založení účtu je Coinbase. Uživatel zde ale nemá přístup k soukromému klíči.

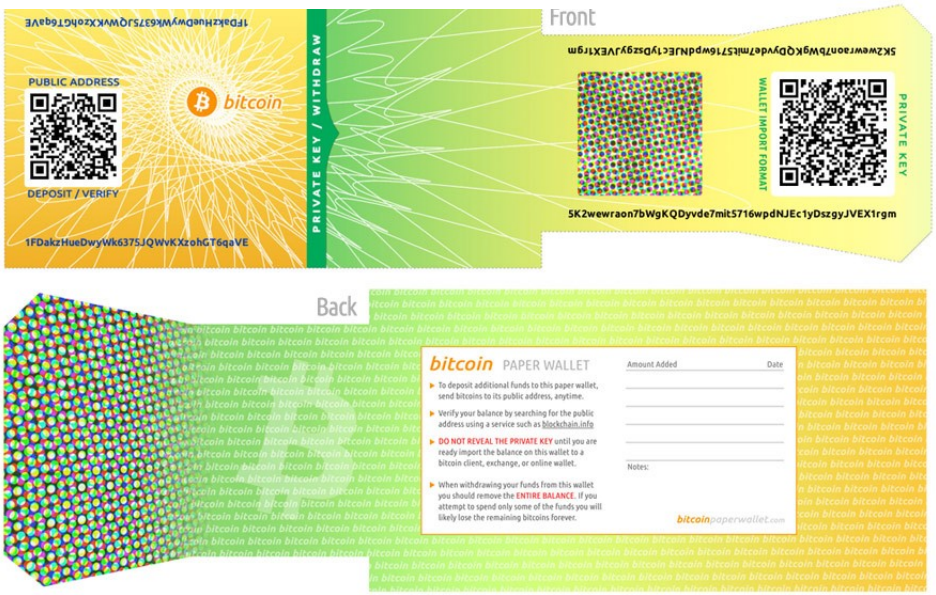
Miksa (2017) uvádí, že kompromisem mezi peněženkami můžou být mobilní aplikace. Primární klíč, který je důležitý k potvrzení transakce, je zašifrovaný v mobilu. Navíc, při založení peněženky uživatel dostane náhodně generovaná anglická slova, která při odcizení telefonu lze použít k obnově peněženky na novém zařízení bez ztráty bitcoinů. Aplikace nezabírá mnoho místa ani nestahuje celý blochchain. Hlavní výhodou oproti ostatním možnostem je fakt, že lidé nosí mobil neustále u sebe, a tak mohou kdykoliv, kdekoliv, kde bitcoiny přijímají, platit.

Podle Fillner (2014) je hardwarová peněženka vhodná pro uchovávání většího množství bitcoinů. Jsou to malá zařízení, která jsou přenosná, dají se připojit k síti, ale většinu svého času zůstávají offline. Díky tomuto faktu jsou jednou z nejbezpečnějších peněženek. Můžeme si je představit jako nějaké USB zařízení, kde je uložený soukromý klíč. Pokud je transakce

prováděna přes počítač, potvrzuje se posléze soukromým klíčem mimo počítač. Mezi nejznámější české značky vyrábějící hardwarové peněženky patří Trezor, který poskytuje navíc zabezpečení ve formě tlačítka na zařízení, které se musí stisknout pro potvrzení transakce.

Poslední možností, ne příliš užívanou, podle Investlus (2018) je uložení bitcoinu do papírové peněženky. Je to pouze papír, na kterém je napsaný privátní klíč. Uživatel si tak z automatů, ze kterých jdou vybrat kryptoměny, může vybrat bitcoiny ve formě papírové peněženky. Nevýhodou je, že do jedné peněženky nelze vložit víckrát bitcoiny. Pokud by uživatel chtěl převést online bitcoiny do papírové podoby, stačí mu stáhnout program, který by pak offline vygeneroval novou peněženku. Tu je pak možné si vytisknout.

Obr. 3. 2 Papírová peněženka



Zdroj: Becker (2017)

3.1.3 Transakce

Peněženka ve skutečnosti neobsahuje bitcoiny, uvádí Coindesk (2018). Obsahuje pouze adresu, ve které je zaznamenáno všechno o transakcích, které uživatel přijal, nebo odeslal. Tato adresa obsahuje dlouhý řetězec s 34 číslicemi a písmeny. Takové adrese se říká veřejný klíč. Nezáleží na tom, kolik lidí zná tento klíč, protože není tajný. Opakem veřejného klíče je klíč soukromý, který obsahuje 64 znaků. Je nutné, aby zůstal skrytý a bezpečně schovaný. Z každého soukromého klíče lze zjistit veřejný klíč, ale nelze to uskutečnit naopak. Tomuto jevu se říká asymetrické šifrování. Každá transakce, která je poslána, musí být tzv. podepsána soukromým klíčem, jinak není možné platbu provést. Podepisování probíhá vypsáním 64 znaků do své peněženky, která následně pošle digitální podpis do sítě, kde čeká na ověření platby.

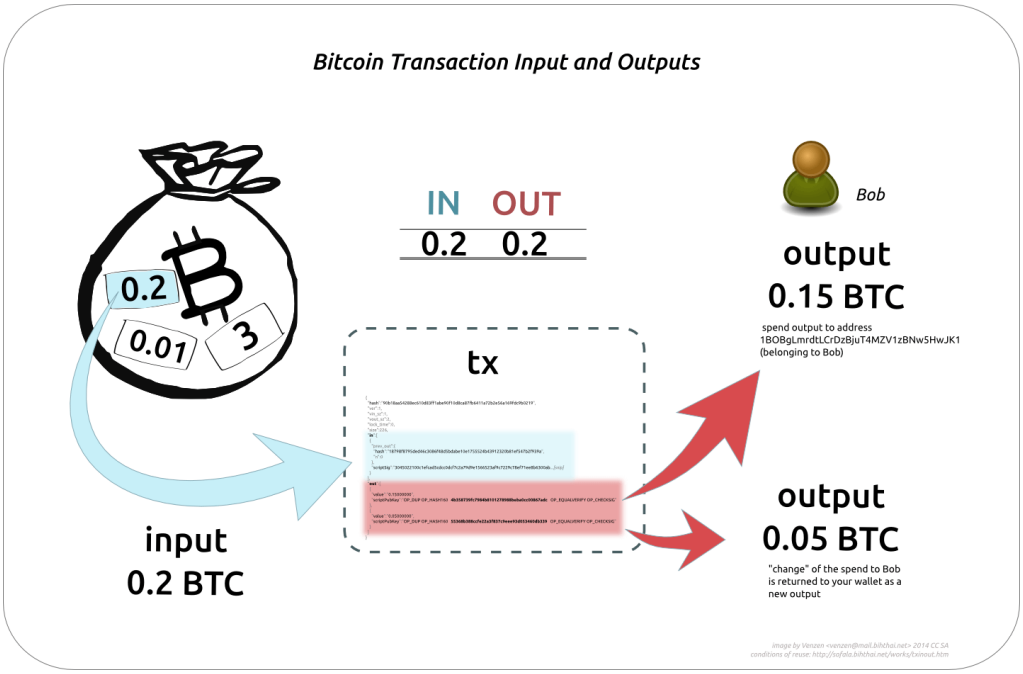
V rámci ověření se zjišťuje, jestli majitel doopravdy bitcoin vlastní a zda jej náhodou nepoužil pro různé platby dvakrát či vícekrát. Až je platba potvrzena, zařadí se do blockchainu jako součást určitého bloku. Potvrzení probíhá vytěžením bloku.

Rychlost transakce závisí na přidání poplatku. Tradearena (2018), tvrdí, že díky velkému množství transakcí je větší poplatek zárukou ověření transakce. Těžaři, kteří transakce potvrzují, si vybírají podle velikosti odměny, které z nich ověří. Pravděpodobněji se rozhodnou pro platbu s větším poplatkem než tu, kde není přidaný poplatek žádný. Může se tak stát, že některé transakce nebudou ověřeny nikdy, jelikož k nim nebyl přiložen žádný poplatek navíc. Délku platby dále ovlivňuje omezení počtu transakcí, které se do jednoho bloku vlezou, průměrná doba, za kterou je jeden blok vytěžený, i velká popularita platebního systému Bitcoin. Průměrná doba vytěžení bloku trvá až 10 min, a proto je jasné, že kapacita momentálně není optimální a nestačí pro plynulý průběh transakcí. Navíc, aby potvrzení bylo doopravdy bezpečné, dohodla se komunita, která užívá bitcoin, že za ověřené platby bude považovat tu, po které následuje v blockchainu ještě dalších 6 ověřených bloků. Z toho vyplývá, že potvrzení by trvalo minimálně jednu hodinu i déle. Tato skutečnost je pro každodenní placení velmi nepraktická a u malých plateb se i poplatky navíc rozhodně nevyplatí. Proto je snaha o rozjetí technologie Lightning Network, která by měla fungovat jako platební kanál. Do takového kanálu může vstoupit několik uživatelů, jenž si navzájem posílají platby. Jakmile je kanál uzavřen, výsledné hodnoty se zapíšou do blockchainu. Výhoda spočívá v tom, že pokud proběhlo několik plateb mezi restaurací a ostatními zákazníky, tak se na konci do blockchainu zaznamená pouze výsledná suma všech plateb jako jedna platba. Tato technologie už z části funguje a používá se, ale je třeba ji ještě rozšířit na celou Bitcoinovou síť. Díky platebnímu kanálu bude možné používat bitcoiny pro každodenní placení. Výhodou bude rychlost a nízké poplatky.

Podle Khaosan (2014) jsou důležitou součástí pro pochopení průběhu transakce tři pojmy. Výstup, vstup a změna. Výstup jsou částky bitcoinu, které jsou poslány od původního majitele a jsou přijaty do peněženky, kde se uchovávají jako nevyčerpané transakční výstupy ve zkratce UTXO. Částky se v peněžence nesčítají, nýbrž jsou zachovány odděleně. Takový transakční výstup je možné odemknout privátním klíčem, jenž je přidružen k adrese příjemce. Pokud jsou v peněžence člověka A oddělené výstupy 0,2 BTC a 0,3 BTC a je potřeba poslat člověku B 0,15 BTC, odemkne peněženka soukromým klíčem výstup 0,2 BTC, který použije celý. Tento výstup se stane vstupem pro transakci 0,15 BTC. Jakmile je transakce odeslána člověku B, v jeho peněžence se stává vstup 0,2 BTC opět výstupem. Rozdíl (0,2 BTC – 0,15

BTC) 0,05 BTC se označuje jako změna, která je poslána novou adresou nazpět do peněženky člověka A. Na obrázku 3.2 lze vidět, že pokud je posílána částka 0,2 BTC jinému příjemci, ze vstupu z peněženky se tak stanou dva výstupy. Jeden, který příjme příjemce a druhý, který se vrátí zpět do peněženky jako změna.

Obr. 3. 3 Názorná ukázka vstupu a výstupů



Zdroj: Khaosan (2014)

3.1.4 Blockchain

Je jakási databáze nebo otevřená účetní kniha sdílená všemi uživateli, která uchovává informace o každé platbě či transakci, která proběhla v Bitcoinové síti na internetové stránce blockchain.info. Podle Digiměny (2014) jsou zde zaznamenány všechny adresy a množství bitcoinů, které k dané adrese patří. Samotný blockchain lze přeložit jako řetěz bloků. Blok jakožto jedna stránka účetní knihy, na které je soupis všech transakcí a řetěz, který zajišťuje posloupnost všech bloků za sebou. Tyto bloky jsou na sobě závislé a lze je připisovat pouze na konec řetězce, nikoliv doprostřed nebo na začátek. Zároveň nejdou zaměňovat ani odebírat. V každém bloku je zaznamenáno několik transakcí, které již byly uskutečněny. Jakmile je blok vytěžen, tak je potvrzen pomocí hashe předchozího bloku. Každý blok tak má přesně daný blok předchozí. Blockchain vypadá jako nějaký strom, který se málokdy větví. To se stává pouze tehdy, pokud jsou vytěženy dva bloky ve stejném či podobném čase. Řetěz nadále navazuje pouze na jeden blok, a to na ten, který je nejdelší, tudíž ho bylo nejtěžší spočítat. Ty bloky, které zůstaly rozvětveny a nebyly použity pro pokračování blochchainu, jsou ignorovány. Zároveň jsou potvrzeny pouze ty, které jsou zahrnuty do pokračujícího řetězu. První blok, který

započal řetěz, se jmenuje Genesis blok. Vytěžil ho samotný tvůrce Bitcoinu Satoshi Nakamoto. Na tento blok jsou připojovány další a další bloky, které po vytěžení již nelze změnit.

Termín otevřená účetní kniha podle Bauerle (2017) znamená, že uživatelé můžou do ní libovolně nahlížet a kontrolovat správnost informací. Hlavním pozitivem blochchainu je, že je provozován na základě P2P sítě, neboli sítě klient-klient (rovný s rovným). Na rozdíl od internetové stránky Wikipedie, která používá model klient-server, to znamená, že je stránka provozována jedním centrálním serverem. Tato centrální autorita stránky kontroluje, spravuje a ochraňuje. Pokud by ale byl tento centrální server zničen, například kybernetickými útoky, nebo zakázán vládou, nebylo by možné Wikipedii nadále používat. Technologie blochchain je odlišná, jelikož nepotřebuje třetí stranu pro uskutečnění fungování stránky a s tím spojenými digitálními vztahy. Takováto síť zmenšuje nebezpečí selhání centrálního serveru, jelikož neexistuje. Aby tato síť byla důvěryhodná, musí splňovat autentifikaci neboli ověření identity, a autorizaci tzv. prokázání povolení k platbě. U blockchainu je autentifikace splněna díky vlastnictví osobního (privátního) klíče. Více osobních informací není k transakci nutné vědět a zároveň je uživatel chráněn proti hackerům. Autorizace plateb, tzn. ověření, že uživatel vlastní dostatek peněz, je zajištěna tak, že síť funguje jako P2P síť a tím pádem pro všechny uživatele platí stejná pravidla.

3.1.5 Hash

Faife (2017) uvádí, že funkce hash je matematická operace přepočtu vstupních dat, která mohou být jakkoliv dlouhá, do výstupních dat omezené, pevné a zároveň vždy stejně dlouhé délky (256-bitových čísel). Tento výstup se nazývá hash. Pokud by se vstupní data změnila o jakékoliv písmeno či mezeru, výsledný hash by byl zcela jiný. U Bitcoinu je funkce hash používaná ve spojitosti s ověřováním nových plateb. Vstupem je každá transakce, která nebyla stále ověřena, plus časové značky a odkazy na předchozí blok a výstupem je určitý počet číslic a písmen, jenž začínají přesným počtem nul. V dnešní době je to 18 nul, k nimž lze dospět až po řadě výpočtů. Z tohoto důvodu trvá vypočítání jednoho hashe přibližně 10 min pomocí výpočetních výkonů každého počítače, jenž se těžení zúčastní.

Funkce hash je lineární neboli jednosměrný algoritmus, uvádí Khatwani (2018). Znamená to, že z původnímu vstupu lze vytvořit výstup neboli hash, ale nelze z hashe zjistit původní data. Například pokud byl lidský palec brán jako vstupní data a výstupem by byl otisk prstu, nešlo by pak zpětně z otisku vytvořit opět lidský palec. Hashování se tak často označuje jako digitální otisk. Bitcoin konkrétně využívá hashový algoritmus SHA-256, jenž byl

vymyšlen Agenturou pro národní bezpečnost ve Spojených státech amerických. Náročnost vytěžení pomocí tohoto hashe se mění po každých 2016 vytěžených blocích.

3.1.6 Těžba bitcoinu

Těžení neprobíhá fyzicky, pomocí lopat a dolování mincí v podzemí, ale je to výpočetní matematický proces, který je decentralizovaný a používá se ke dvěma účelům. Jednak se díky těžbě potvrzují a kontrolují transakce uživatelů Bitcoinu za pomocí velkého výpočetního úsilí a jednak vznikají nové bitcoiny s každým vytěženým blokem. Proto je těžba pro funkci Bitcoinu nepostradatelná. Pokud ale bylo řečeno, že je to proces decentralizovaný, znamená to, že neexistuje žádná centrální autorita, která by transakce potvrzovala. Samotné platby si musí uživatelé potvrzovat sami.

Investplus (2016) uvádí, že tuto činnost zajišťují uživatelé, kterým se říká těžaři. Aby však těžaři byli motivování k tomu, aby takto energeticky náročnou těžbu prováděli, jsou za to odměňováni. Předtím, než těžba neboli ověřování transakcí začne, musí se nejprve zaznamenat na síti. To probíhá pomocí ostatních uživatelů, kteří nemusí být nutně těžaři. Transakce, která je na síti pouze ve formě datového souboru, zahrnuje data o příjemcově a odesílatelově adrese a taky množství bitcoinu, jenž bylo odesláno. Jakmile je platba poslána, zaznamenává se u nejbližších počítačů neboli uzlů, které používají rovněž uživatele, kteří jsou připojeni k síti. Jakmile je transakce ověřena jakýmkoliv uzlem, je poslána dál do dalšího nejbližšího uzle. U těchto uživatelů se ověřují pouze formální záležitosti, a to, zda odesílatel doopravdy vlastní napsanou částku. Následně jsou platné platby rozšířeny po celé síti a ty špatné jsou vyřazeny. Pokud se některá platba dostane k těžaři, kromě formálního ověření si ji automaticky uloží do paměti k dalšímu zpracování. Jakmile jich má těžař v počítači dostatek, maximálně o velikosti 1 MB, vytvoří z nich soubor, který se nazývá blok. Do tohoto bloku již nové transakce nadále nevstupují a blok je připravený k těžení. V tomto stádiu nejsou platby stále potvrzené, ani započítané.

Po uzamknutí bloku je zahájena těžba těžařem. Ten používá hashovací algoritmy, díky kterým je blok upravován. Z obrovského množství informací a dat je díky hashovacího algoritmu vytvořen řetěz symbolů, hash. Ne každý vzniklý hash je správný. Tato kryptoměna má určeno, po jak dlouhou dobu budou těžaři hledat správný hash, než blok vytěží. V době psaní této práce trvá vytěžení jednoho bloku přibližně deset minut. Aby nebylo tak jednoduché hash najít, jsou systémem vytvářeny různé požadavky na to, jak má výsledný hash vypadat. Složitost se odvíjí podle počtu těžařů a jejich výpočetní techniky. Jedním z častých požadavků

je hash, ve kterém jsou na prvních místech obsaženy nuly. Aby těžař docílil toho, že se změní jeho výsledný hash na jiný požadovaný, musel by změnit vstupní data. To by znamenalo, že by se musela změnit data ve vstupních transakcích. Jelikož to však celý platební systém Bitcoin nepodporuje, používá se tzv. proof of work (důkaz o práci).

Acheson (2016) uvadí, že dříve, než těžař zahájí těžbu pomocí programu, zahrne do vybraného bloku tzv. nonce. Tento nonce je tvořen pouze libovolným textem, který může obsahovat nějaké číslice. Neovlivňuje nijak transakce, pouze výsledný hash. Program, který si těžař zvolil k těžení, dokáže tento nonce několikrát za sekundu změnit, aby docílil výsledného požadavku na hash. Ve zkratce k výslednému hashi slouží jako vstupní data hash předchozího bloku, transakce aktuálního bloku a nonce, který jako jediný dokáže změnit výsledek. Nonce je pokaždé nějaké celé číslo mezi 0 a číslem 4294967296. Počítač během nalézání správného nonce musí vypočítat až 10^{21} výpočtů, proto nyní zpravidla trvá najít správný hash přibližně 10 min. Dále rychlost záleží na výkonnosti počítače či zvoleném hardwaru. Důkaz o práci tak dokazuje, že zde účastníci vynaložili velkou výpočetní sílu, než na požadovaný výsledek v určitém rozsahu přišli.

Coindesk (2018) uvádí, že výsledný hash musí začínat určitým počtem nul, momentálně osmnácti nulami. Je nemožné předem vědět, které číslo jako nonce hned vybrat, jelikož dvě po sobě jdoucí čísla tvoří naprosto jiný výsledný hash. Navíc může existovat několik čísel, která budou splňovat požadavky osmnácti nul, nebo žádné. Jakmile je nalezen správný hash výherním těžařem, pošle výherce správný výsledek ostatním těžařům, kteří jeho blok i s hashem v krátké době ověří. Pokud je výsledek správný a ověřený, je tento blok zařazen do blochchainu. Těžař, jehož počítač správně vypočítal danou hodnotu hashe, dostává jako odměnu nové bitcoiny, které pro každý uhodnutý blok v době psaní činí 12,5 BTC.

Těžení se stává čím dál rychlejším díky přibývajícímu hardwaru, který urychluje výpočetní operace. Postupem času uvádí Bicoin-info (2016), že lze těžit pomocí:

- procesoru,
- grafické karty,
- ASIC jednotky.

Původní myšlenkou tvůrců Bitcoinu bylo, že potvrzovaní transakcí bude moci provést jakýkoliv uživatel doma na svém počítači díky procesoru. I v dnešní době je možné pomocí svého počítače těžit, ale jednak se to energeticky nevyplatí, respektive člověk zaplatí více za elektřinu, než dostane bitcoinů a jednak je šance na zjištění správného hashe takřka nulová.

Ze začátku bylo těžení uživatelsky přívětivé. Uživatelé, kterých nebylo mnoho, ověřovali transakce z pohodlí domova a vytěžení jednoho bloku nebylo až tak energeticky náročné. Postupem času, kdy se o Bitcoinu dovídalo stále více lidí, konkurence v těžení přibývalo. Byly používány stále výkonnější počítače, dokud se nepřišlo na to, že herní grafické karty jsou mnohem výkonnější a rychlejší pro vypočítávání hashů než dřívější procesory. Používaly se grafické karty značky AMD, se kterými se těžilo docela dlouho. V dnešní době se těží na specializovaném hardwaru ASIC, který je určen přímo pro těžbu. Tento hardware je udělán tak, aby měl co největší výkon a co nejnižší spotřebu. Dlouhou dobu již jsou stavěny obrovské farmy převážně v Číně, které shromažďují těžební hardwary a usazují se tam, kde je levná elektřina, dostupnost hardwarů a vhodné, chladné klima.

Těžařské pooly

Poslední novinkou ohledně těžení jsou pooly. Těžařský pool je uskupení těžařů, kteří se rozhodli spolu těžit. Výhodou je, že dohromady mají daleko větší šance na vyřešení správného hashe, než kdyby ho těžař hledal sám. Pokud někdo z poolu vyřeší správně hash, rozdělí si všichni odměnu 12,5 BTC mezi sebe. Jedná se tak o nízký trvalý příjem. Pokud by se těžař rozhodl těžit sám za sebe, nemusel by celý život nic vydělat, anebo by naopak mohl vyřešit správně hash a mít celých 12,5 BTC pro sebe. Avšak díky současné obtížnosti je výhra téměř nemožná. Je důležité, aby žádný pool nezískal víc než 51 % výpočetní síly v síti. V tomto případě by v síti nastal zmatek. První těžařský pool, shodou okolností český, vznikl na konci roku 2010. Založil jej Marek Palatinus a jmenuje se Slush Pool.

3.1.7 Výhody a nevýhody Bitecoinu

Za hlavní výhody uvádí Fillner (2014) decentralizaci kryptoměny, díky které nedochází k žádné kontrole vládou, centrálními bankami a jinými autoritami. Dále Bitcoin nepodléhá inflaci, nelze nijak devalvovat, intervenovat nebo jakkoliv tisknout, je to spíše měna deflační. Dalším kladem je, že je nemožné kryptoměnu zfalšovat, jelikož všechny platby jsou kontrolovány celou sítí. Aby bylo možné utratit jedny peníze víckrát, musel by kdokoliv vlastnit více, než 51 % výkonu celkové sítě Bitcoin. V dnešní době toho mohou docílit těžařské pooly, ale tato hranice překročení je silně kontrolována. Zároveň ani pooly tento limit nechtějí překročit, jelikož by Bitcoin pozbyl důvěry a měna by pravděpodobně ztratila svou hodnotu. Za další klad je pokládána anonymita neboli lépe řečeno pseudonymita. Za jednu z posledních výhod lze označit jednotnou měnu, která je stejná jak v Evropě, tak v Americe a není ji třeba jakkoliv směňovat do jiné měny. Za poslední uvedené pozitivum je možné označit fakt, že se

systém Bitcoinu nemůže zhroutit. Každý uživatel, který buď kryptoměnu těží, nebo vlastní softwarovou peněženku, disponuje s uloženými kopiemi všech proběhlých transakcí, jinak řečeno s blockchainem. To znamená, že i kdyby se stala jakákoliv pohroma a zbyl by na světě pouze jeden počítač, který by fungoval, kryptoměna by tak nadále po rozeslání stavu účtů mohla fungovat. Za časté zmiňované nevýhody naopak autor uvádí nutnost mít internet. Bez internetu není možné si bitcoiny cokoliv koupit. Následující velkou nevýhodou jsou krádeže. Například pokud uživatel používá jednoduché heslo své peněženky, tak je možné, že mu nějaký hacker veškeré bitcoiny odcizí. Dalším mínusem nejen Bitcoinu je velká volatilita. Je možné, že jeden den se hodnota srazí na polovinu, jindy zas cena bitcoinů poroste obrovskou rychlostí. Za největšího nepřítele kryptoměn dnešní společnost pokládá politiku, vládu a vyšší pozornost. Pokud je kryptoměna více a více používána, znamená to pro banky, že jejich platební systém je čím dál více v ohrožení. Centrální autority se tak snaží v některých částech světa kryptoměny regulovat a díky tomu bývá kurz často ohrožen. Jsou ale i výjimky, například Japonsko, které k Bitcoinu má pozitivní postavení a již této kryptoměně přidělilo statut měny.

3.2 Ethereum

Podobně jako Bitcoin je Ethereum kryptoměna, která funguje jako decentralizovaná měna, jež používá technologie blockchain. Dle Ethereum (2018) ve srovnání s Bitcoinem, jsou si ze začátku obě kryptoměny podobné. U obou jde o decentralizovanou měnu, tvoří bloky, jsou uloženy do blockchainu a jsou ověřovány těžaři, kteří za vytěžení bloku dostávají odměnu. Avšak Ethereum využívá blockchain i ke spouštění otevřených přístupných zdrojových kódů u tzv. chytrých kontraktů. To znamená, že spravuje inteligentní smlouvy čili aplikace, které byly vytvořeny tak, aby se nedaly cenzurovat, odstavit, podvést apod. Dříve než bude blíže popsáno Ethereum, je nutné si uvést funkci internetu.

Hertig (2017) popisuje, že na internetu je uloženo mnoho naších osobních údajů, hesel či informací o našich financích. Tyto údaje spravují společnosti typu Google nebo Facebook a jiné. Nabírají pracovníky, kteří se snaží zabezpečovat jejich stránky a údaje, které patří nám. Jelikož jsou tyto servery vlastněny třetí stranou, je možné, že naše údaje budou zneužity, ukradeny nebo změněny hackery nebo dokonce vládou. Ti získají přístup k těmto datům prostřednictvím ovlivnění či zaútočení na vlastníky serverů. Ethereum se tak připojilo k názorům, že centralizovaný internet je hřích a stalo se tak jednou z posledních technologií, která pracuje na bázi decentralizace. Snaží se fungovat jako decentralizovaný obchod s aplikacemi. Na rozdíl od Bitcoinu, který používá blockchain čistě k transakcím, Ethereum používá blockchain k nahrazení třetí strany internetu. Je zde používán model tzv. světový

počítač. Co znamená, že všechny servery jsou zde nahrazovány uzly, které spravují uživatelé na počítači po celém světě. Každá změna (i například změna programu), která je zaznamenána v síti Etherea, je spojována do bloků, ze které stejně jako u technologie Bitcoinu vznikne blockchain. V běžném životě si lidé například vybírají aplikace, které si chtějí stáhnout a zároveň jsou v těchto aplikacích uloženy informace o kreditní kartě, historie všech nákupů a jiných informací, které kontrolují třetí strany. Zároveň nám můžou některé servery úplně odepřít přístup. Ethereum oproti jiným serverům funguje na principu vrácení kontroly dat vlastníkovi a vlastních práv autorovi. Výsledkem je neexistence kontroly třetí osoby nad vlastníkovými údaji a odepření přístupu. Pokud tedy uživatel provede v aplikaci nějaké změny, přidá či odebere poznámky, každý uzel v síti zároveň provede změnu. Není však dodnes jasné, které aplikace jsou díky blockchainu užitečné a lepší než ty, co používáme dnes.

Aby takováto síť mohla fungovat jako obchod, je potřeba zde platit nějakou měnou. Alza (2018) uvádí, že jedinou měnou, za kterou je možné si aplikace i jejich změny nakoupit, je ether, který se rovněž může značit zkratkou ETH a je volně směnitelný. Ether se zde, spíše než digitální měna, označuje jako palivo, které vývojáři musí zaplatit. Následně těžaři provedou změnu, úpravu či odstranění části programu, za co jsou posléze odměněni ethery.

3.2.1 Vznik Etherea

První nádech Ethereu dal rusko-kanadský vývojář Vitalik Buterin. Dle Hertig (2017) se tento programátor se nejprve nechal inspirovat Bitconem a zároveň byl jedním z lidí, kteří se o běh Bitcoinu zasloužili. Později přemýšlel nad možností využití blockchainu ve větším měřítku, než bylo pouhé ověřování plateb. Roku 2013 napsal knihu, ve které byla popsána alternativa platformy, která by mohla vést ke vzniku decentralizovaných aplikací. Tento systém byl pojmenován Ethereum. Dalším spoluzakladatelem se stal Gavin Wood, který napsal knihu o virtuálním stroji EVM, díky kterému je dnes Ethereum umožněno fungovat. V červenci roku 2014 byla vytvořena kampaň na podporu vzniku platformy, kde si lidé mohli zakoupit kryptoměnu ether. Tato kryptoměna slouží k funkci akcií v tomto projektu. Následně 30. července 2015 se síť rozběhla a je určena vývojářům pro tvoření svých decentralizovaných aplikací.

3.2.2 Chytré kontrakty

Existují dva druhy účtů v síti Ethereum, uvádí Investplus (2018). První účty se jmenují vlastněné účty se zkratkou EOA. Tyto účty jsou označovány jako běžné uživatelské účty. Díky nim je možné do systému vložit chytrý kontrakt, jinak řečeno cloudový účet CA, což je druhý

typ účtů. Tyto CA vlastní svou adresu a je zde možné odesílat a přijímat kryptoměnu ether. Tyto vzniklé programy jsou zaznamenány v blockchainu a jsou zpřístupněny všem uživatelům. CA jsou zaktivovány po dobu, dokud není splněna určitá podmínka, nebo dokud není veškeré palivo (ethery) vyčerpáno. Vývojáři, kteří CA vytvořili, musí na něj nahrát palivo. Aby totiž cloudové účty byl funkční, potřebují ke svému chodu výpočetní výkon, který provádí těžaři na svých počítačích. Jakmile těžař získá signál ke změně či aktivaci programu, provede těžbu, za kterou získá odměnu v podobě paliva a daný úkon provede. Mezi nejznámější CA patří aplikace Slock.it. Díky ní je možné prodávat, sdílet či pronajímat různé věci.

3.2.3 Těžba

Stejně jako u Bitcoinu je používána těžba etherů k ověřování transakcí kryptoměn. Jakmile tedy uživatel pošle ethery na adresu určitého cloudového účtu, aby jej aktivoval, těžaři provedou těžbu tzv. ověření transakce. Ti vlastní program, jenž napomáhá k řešení výpočetních operací, díky kterým jsou transakce převáděny do krátkého kódu tzv. hashe. Ethereum používá hashovací funkci Ethash. Na rozdíl od hashe SHA-256, který používá Bitcoin, je možné hash Ethash zpětně rozšifrovat na původní informace. To umožňuje zachování veškerých informací. Jelikož není těžba zadarmo a je při ní spotřebováno mnoho energie a hardwaru, je správné řešení oceněno 5 ethery za jeden blok. Každý blok je vytěžen cca každých 12 sekund, uvádí Investplus (2018).

3.2.4 Výhody a nevýhody kryptoměny

Na rozdíl od množství bitcoinu nemá ether omezené množství. Kladným rozdílem mezi sítí Bitcoinu a Etherea je rychlost vytěžení jednoho bloku. Zatímco těžení jednoho bloku u Bitcoinu trvá cca 10 minut, Ethereum stíhá vytěžit blok za pouhých 12 sekund. Z tohoto důvodu je potvrzení platby u etheru mnohem rychlejší a nevznikají zbytečné komplikace, které jsou v dnešní době řešeny u platby s bitcoinem. Navíc je již vytěženo přes dvě třetiny bitcoinů, které patří prvním těžařům oproti etheru, kde bude vytěžena půlka veškerého množství až v roce 2020. Těžba etherů je prováděna stále pomocí grafických karet a může být stále pro jednoho těžaře výnosná, uvádí Alza (2018).

Obdobně jako u ostatních kryptoměn jsou i zde rizika spojená s volatilitou měny. Hodnota etherů je spjata s důvěrou uživatelů a není nijak podložena. Avšak i tradiční měny, jak uvádí Investplus (2017), nejsou podle mnoha zastánců kryptoměn něčím podloženy. Dále není kryptoměna regulována třetí stranou, a proto je častokrát během dne zhodnocena či znehodnocena. Následujícím rizikem může být i méně časté vykrádání burz a směnáren,

jež s kryptoměnami obchodují. Toto riziko lze eliminovat tím, že si uživatel své ethery uloží do hardwarové peněženky, nebo jiné softwarové peněženky, která ke své funkci nepotřebuje burzy. Za nevýhodu lze také pokládat fakt, že Ethereum není tak známé jako Bitcoin a je komplikovanější. To může mít za následek menší množství uživatelů, kteří danou kryptoměnu využívají. Navíc mnoho lidí tvrdí, že Ethereum neberou jako klasickou kryptoměnu, ale spíše jako zajímavou technologii.

3.3 Litecoin

Je digitální měnou, kryptoměnou, která podle Investplus (2018) byla vytvořena v říjnu roku 2011 inženýrem Charlesem Lee. Je navržena jako napodobenina první kryptoměny Bitcoin. Oproti Bitcoinu je vylepšena rychlost potvrzení transakce, která je 4x větší. Čtyřikrát větší je i celkové množství, které je možné maximálně vytěžit, a to představuje 84 milionů litecoinů (jednotka kryptoměny). Díky tomuto se do sítě ukládá čtyřikrát více dat. Litecoin využívá decentralizovanou síť, která je založena na technologii klient – klient. Obdobně jako kryptoměny, které jsou popsány výše, tak i Litecoin aplikuje technologii blochchainu. Jeden blok, ve kterém jsou obsaženy informace o proběhlých transakcích a datech předešlého bloku, je vytěžen za 2,5 minut a odměna pro výherního těžaře činí 25 LTC. Rozdílný je i hashovací algoritmus, označován jako Scrypt. Velkou výhodou Litecoinu jsou poplatky za transakce, které se pohybují v tisícinách nebo setinách litecoinů. V porovnání s Bitcoinem je to obrovský rozdíl, jelikož poplatky za provedení transakce se u Bitecoinu neustále zvyšují a v přepočtu na české koruny dokážou vyšplhat na desítky nebo stovky korun.

3.3.1 Výhody a nevýhody Litecoinu

Jak již bylo napsáno, výraznou výhodou oproti Bitcoinu je rychlost potvrzení transakce. Jenže tahle výhoda má rovnou i nevýhodu. Investplus (2018) tvrdí, že díky rychlejšímu těžení se ukládá do blockchainu více dat, která zabírají více místa. Také kvůli menšími počtu těžařů a rychlejšímu potvrzování zbývá méně času na tak kvalitní zabezpečení, jako má Bitecoin. Stejně jako většina ostatních kryptoměn, není ani Litecoin podložený a jeho hodnota je určena pouze trhem nabídky a poptávky. Za další nevýhodu lze uvést menší popularitu oproti Bitcoinu, která vede k menšími počtu uživatelů a obchodníků, kteří platbu v litecoinech přijímají.

4 Zhodnocení kryptoměn se zaměřením na Bitcoin

Tato kapitola je zaměřena na konkrétní tři kryptoměny. Primárně je zkoumán Bitcoin, který je z nich nejstarší, nejznámější a zároveň nejrozšířenější. V první části kapitoly jsou porovnávány funkce tradičních měn s funkcemi Bitcoinu a jiných kryptoměn, kde pro tuto práci je vybrán Litecoin a Ethereum. Díky sběru dat a zobrazení pomoci grafu lze následovně podložit, zda kryptoměny plní základní rysy tradičních peněz, jako je prostředek směny, zúčtovací jednotka a uchovatel hodnoty. A dále, jestli je možné, aby tyto měny v budoucnu mohly nahradit klasické fiat měny. Druhá část poslední kapitoly se zabývá jak pozitivními, tak negativními faktory, které by mohly budoucnost kryptoměn ovlivnit. V kapitole 4.2 je zjišťován stav technologií, které by mohly zrychlit transakce a přitáhnout tak pozornost více uživatelů. Poté je brán zřetel na regulaci vlád, které mají buď negativně vyhraněný názor, nebo naopak podporují tuto poměrně novou netradiční měnu. Nakonec je mezi tuto část zařazeno velké napadení burz, jenž ovlivňují budoucnost a důvěryhodnost kryptoměn.

4.1 Zhodnocení funkcí tradičních peněz aplikované na kryptoměny

Pokud je možné, aby kryptoměny v budoucnosti nahradily funkci tradičních měn, je třeba nejprve zanalyzovat, zda kryptoměny vůbec plní funkci klasických měn. Tyto skutečnosti jsou zjišťovány díky empirickým charakteristikám statických souborů. Pro množinu souborů jsou v této práci použity data ohledně výšky kurzu kryptoměn, zlata a jedné tradiční měny (EUR/USD), dále data počtu transakcí za den, a jiných. Charakteristiky jsou zde použity jak polohové, kvůli zjištění aritmetického průměru, tak variabilní, kvůli určení rozptylu, směrodatné odchylky a variačního koeficientu souboru. Díky tomu je možné určit, nakolik je měna volatilní a zda je tedy vhodná jako zúčtovací jednotka. Dále je v této části použito měření závislosti, konkrétně závislosti lineární. Pro tuto závislost je aplikovaný Pearsonův korelační koeficient, díky kterému je možné zjistit například společná průběh kurzu a počtu transakcí za den a jiných. Také je v této části mnohdy využito různých ročních či kvartálních procentních vyjádření růstu či poklesu měn, míst k placení apod.

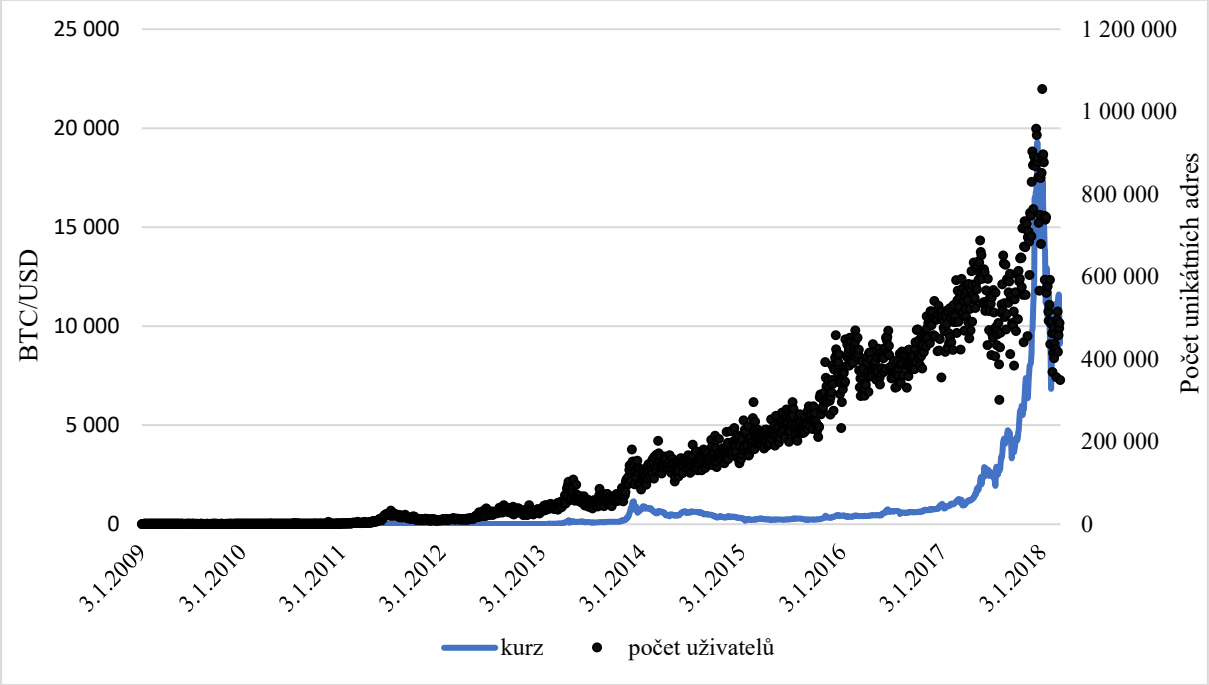
4.1.1 Kryptoměny jako prostředek směny

Základním rysem tradičních peněz, které fungují jako prostředek směny je důvěryhodnost. K zjištění stoupající či klesající tendenci důvěryhodnosti, je třeba určit, jakým směrem roste počet uživatelů. A to jednak skrz uživatele, kteří by si za kryptoměny něco chtěli nakoupit, a jednak skrz uživatele, kteří jsou ochotni kryptoměnu přijmout a něco za ni poskytnout.

Počet uživatelů, kteří BTC používají

U kryptoměn není jednoduché zjistit, kolik uživatelů ji používá, a to z důvodu anonymity. Ale lze ji přibližně zjistit pomocí unikátních adres, které se vyskytují v blockchainu v den, kdy bitcoin nějaká adresa přijala, nebo odeslala. Mohou se zde ale vyskytovat nepatrné odchylky z důvodu, že jeden uživatel může vlastnit více unikátních adres, které jsou vesměs nedohledatelné k původnímu majiteli, a tak uměle navyšovat počet uživatelů. Avšak i v dnešním světě kreditních karet může jeden člověk vlastnit více účtů. Na obrázku 4.1 je ukázán vývoj mezi hodnotou kurzu a počtem uživatelů za den. Dále je možné vidět, že do roku 2017 jak hodnota kurzu, tak počet uživatelů přibýval. Od roku 2018 mají oba dva ukazatele klesající tendenci.

Obr. 4. 1 Vývoj kurzu a počtu uživatelů za den (2009-2018)



Zdroj: Blockchain.info (2018), vlastní úprava

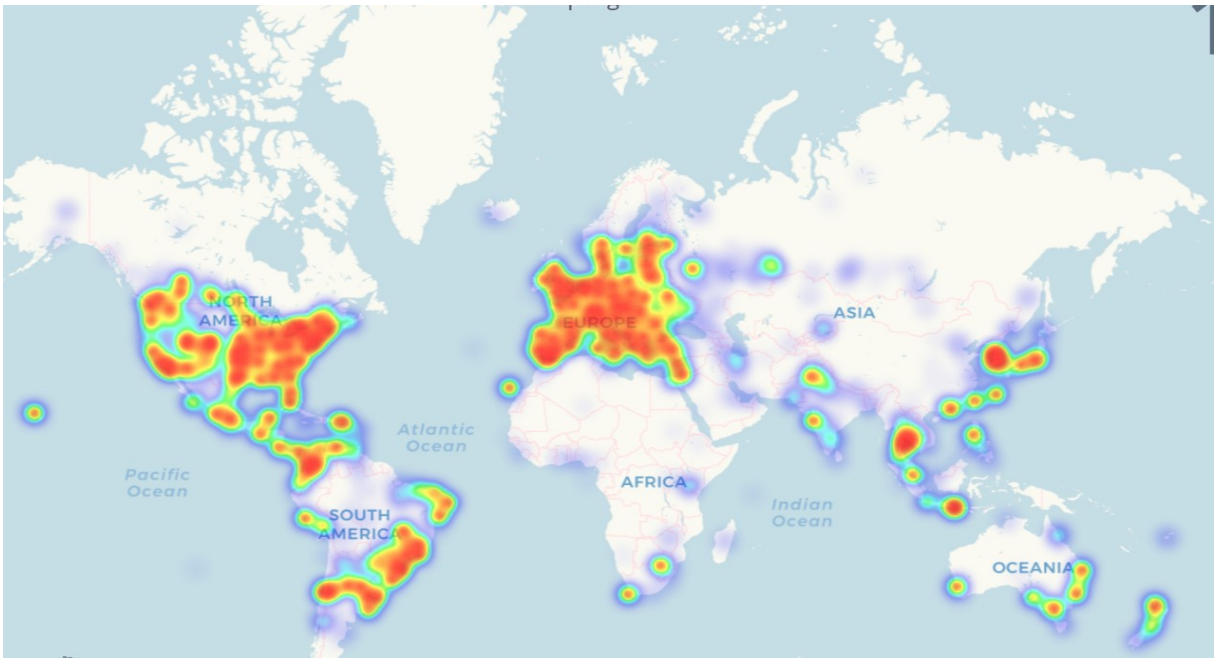
Vývoj mezi dvěma veličinami se dá měřit pomocí koeficientu závislosti. Tento koeficient podle Šalounová (2013) patří mezi ukazatele, které ukazují na lineární závislosti. Obvykle se znázorňuje pomocí grafu, kde se jedna proměnná sestrojí jako přímka, či spojitá čára a druhá proměnná se zakreslí jako shluk bodů. Pokud se body na výsledném grafu shlukují poblíž přímky, je zde možné uvažovat o potenciální závislosti. Následně se dá domněnka potvrdit pomocí matematického výpočtu korelačního koeficientu (r_{xy}):

$$r_{xy} = \frac{s_{xy}}{s_x s_y}, \tag{4.1}$$

kde s_{xy} je kovariance proměnných *x, y*, s_x je směrodatnou odchylkou proměnné *x* a s_y je opět směrodatná odchylka, ale proměnné *y*. Koeficient může nabývat hodnoty od -1 do 1. Pokud je výsledná hodnota r_{xy} větší než nula, jedná se o přímou lineární závislost. V opačném případě se jedná o nepřímou korelační závislost. Pokud je výsledkem 0, znamená to, že zkoumané znaky jsou na sobě nezávislé.

Pearsonův korelační koeficient mezi kurzem a počtem uživatelů za den udává hodnotu 0,663. Jelikož je to hodnota vyšší než 0, jedná se o přímou závislost. Navíc se hodnota vyskytuje v mezích ⟨0,5; 0,7), a to udává, že se jedná o závislost významnou. Lze tedy na základě těchto dat a výpočtů tvrdit, že hodnota kurzu i denní počet uživatelů mají významný společný průběh. A jelikož se jedná o závislost přímou, tak je možné, že pokud uživatelů přibývá, tak zároveň roste i hodnota kurzu a naopak.

Obr. 4. 2 Místa, kde se dá platit BTC (březen 2018)



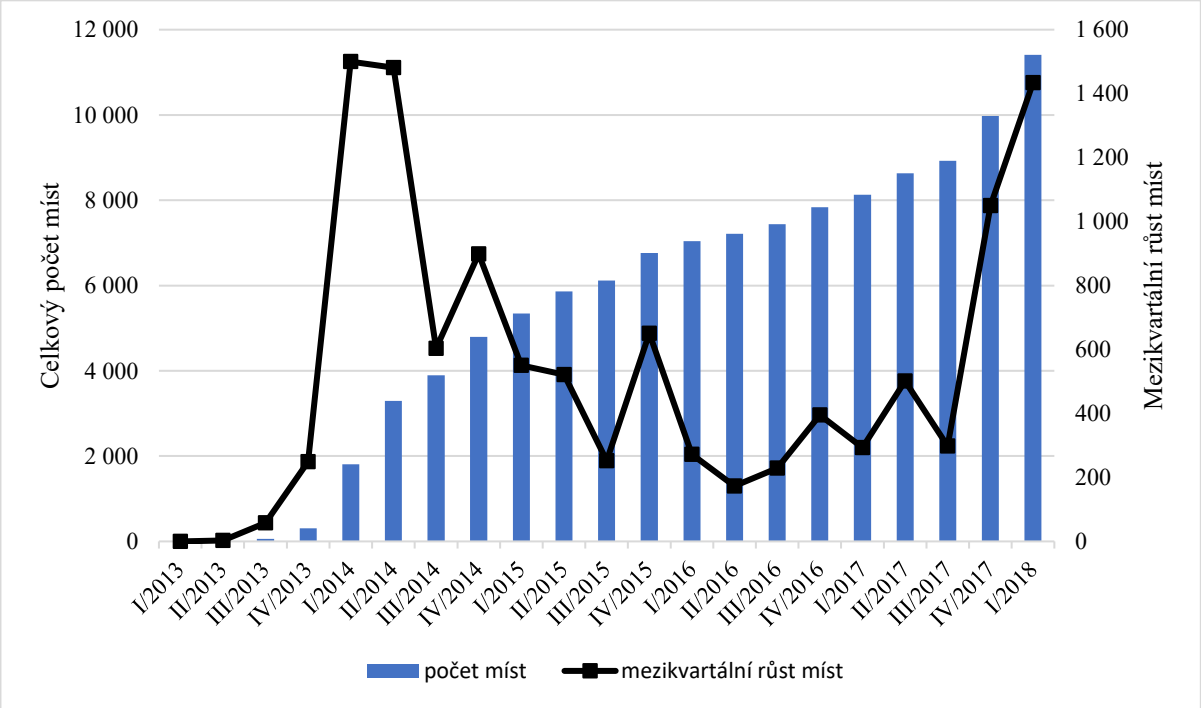
Zdroj: Coinmap (2018)

Coinmap (2018) uvádí, že na světě existuje k datu 14.3.2018 celkem 12 048 registrovaných míst, kde se dá platit bitcoiny. Nejvíc obchodů či institucí, které přijímají bitcoin, se vyskytuje v Severní Americe a Evropě. Oproti tomu nejmenší počet obchodníků se nachází v Africe a v Austrálii a Oceánii. Přímo litecoiny se dá zaplatit hodně produktů jako jsou oblečení, jídlo, pití, letenky aj. Stránka Litecoin (2018) uvádí obchody jako Bitcoin Shop,

Coinplay (hry), Crypto Pet (pro domácí mazlíčky), All Things Luxury (šperky), San Marco Coffee a mnoho dalších.

Na obrázku 4.3 je pomocí sloupců znázorněno, jak stoupá počet míst ve světě, kde se dá platit bitcoiny. Černá spojnicová čára ukazuje, kolik míst přibylo za každé čtvrtletí v jednotlivém roce. Největší růst počtu míst nastal v I. čtvrtletí v roce 2014, následně i v II. čtvrtletí 2014. Od té doby stoupalo tempo růstu míst pomaleji až do konce roku 2017. Od té doby množství míst, kde přijímají bitcoiny, výrazně přibývá. Celkově lze tvrdit, že nejvíce míst přibývá na konci a na začátku roku. Závěrem výskyt míst stále stoupá, ukazuje to tak na důvěryhodnost kryptoměny a plnění funkce prostředku směny.

Obr. 4. 3 Mezikvartální růst míst, kde se dá platit BTC (2013-2018)



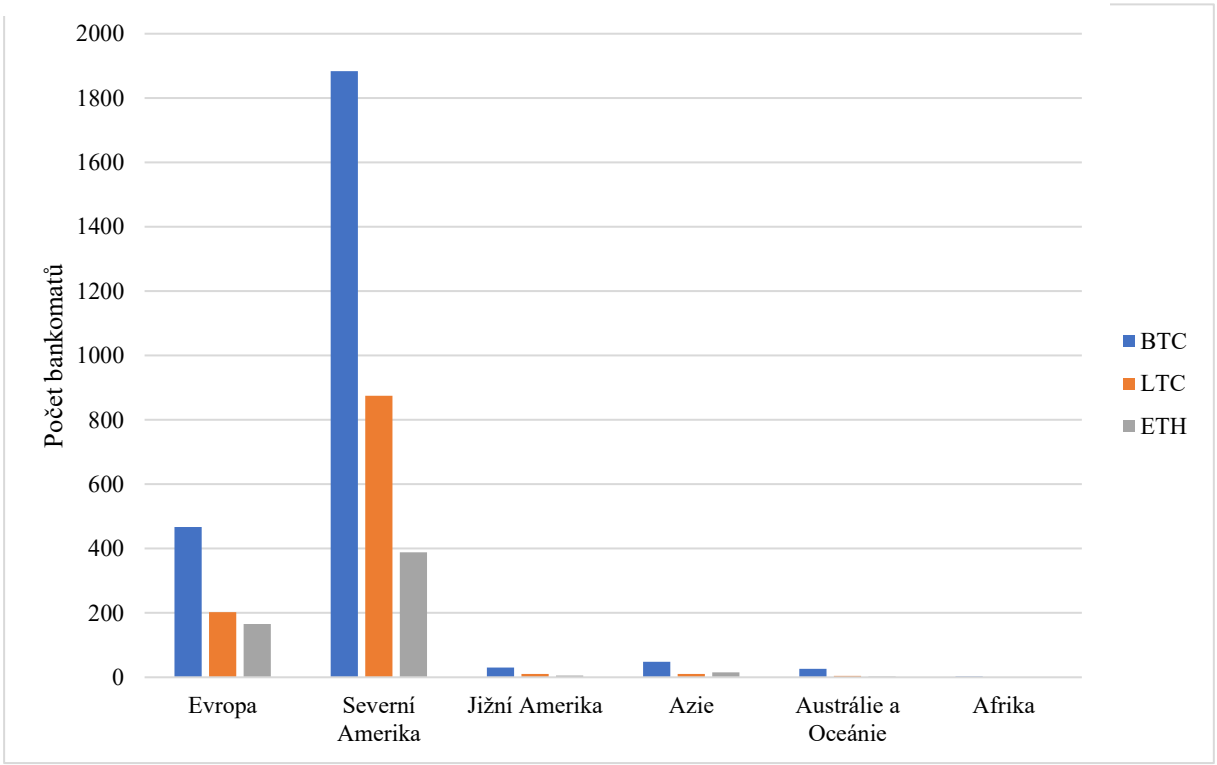
Zdroj: Coinmap (2018), vlastní úprava

S počtem míst zároveň souvisí zvyšování počtu bankomatů, kde se kryptoměny dají buď koupit nebo prodat. Bitcomat (2018) vysvětluje, že se jedná o tzv. bitcoinové bankomaty, ze kterých se kromě bitcoinů, dají vybrat i jiné altcoiny. Pojem altcoiny je odvozen od slova alternativní coiny. Autor tak má na mysli ostatní kryptoměny, vyjma bitcoinů. Bankomaty fungují jako směnárny, kde se dá směnit hotovost za digitální měnu a naopak. Aby mohl automat fungovat s aktuálním kurzem, který se stále mění, je propojen s nějakou určitou burzou. Pokud uživatel nakupuje kryptoměnu, vloží fiat peníze do slotu pro peníze a buď mu vyjede papírová peněženka s adresou, klíči a částkou, nebo se peníze zašlou na email

v zašifrované podobě, anebo si je uživatel jednoduše načte na QR kód svojí bitcoinové peněženky, který má buď vytištěný nebo uložený v mobilu. Pokud je bitcoin prodáván, je nutné k bankomatu zajít dvakrát. Poprvé si člověk zvolí částku, kolik bitcoinů prodává a nechá si vygenerovat příkaz k platbě. Následně načte svou bitcoinovou peněženku, kde se suma BTC odečte. Po zhruba půlhodině, kdy se je transakce 3x ověřena (z důvodu vlastností ověření transakcí pomocí těžařů), je možné opět zajít k bankomatu a pomocí QR kódu příkazu vybrat částku v hotovosti.

Na obrázku 4.4 je možné vidět výskyt bankomatů v jednotlivých kontinentech, ze kterých je možné nakoupit nebo prodat bitcoiny, litecoiny a ethery. Je zřejmé, že nejstarší a nejznámější kryptoměna má zároveň největší počet automatů a naopak Ethereum, které je nejmladší z tří vybraných kryptoměn, má bankomatů nejméně. Severní Amerika i Evropa mají podle obrázku nejvřelejší vztah k digitálním měnám, oproti Africe nebo Jižní Americe. Tato skutečnost může být dána i chudobou, nepříznivými podmínkami, typem vlády, špatným přístupem k internetu i jinými faktory.

Obr. 4. 4 Výskyt bankomatů na kryptoměny (březen 2018)



Zdroj: Coinatmradar (2018), vlastní úprava

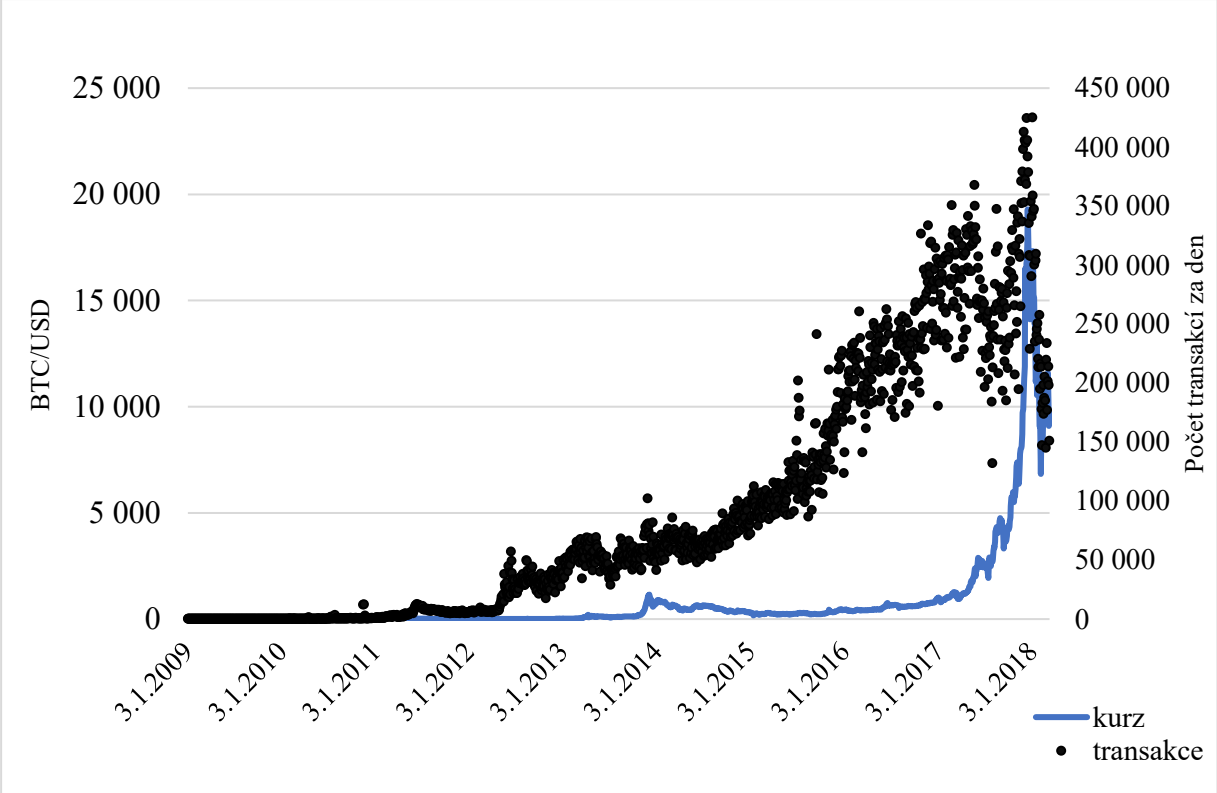
Z hlediska zvyšujícího se výskytu míst i počtu bankomatů je možné trdit, že kryptoměny plní funkci prostředku směny, ale jenom částečně na určitých místech. Jinou hodnotu má tato funkce například v Severní Americe v New Yorku, a jinou v Africe, kde je takřka nulová.

Bez rozšíření do všech oblastí tak nemají kryptoměny pozitivní vyhlídky na budoucí nahrazení klasických měn.

Počet transakcí

S prostředkem směny samozřejmě souvisí i transakce a to, kolik jich přibližně proběhne za den oproti fiat měnám. Na základě předchozího obrázku 4.2 je doloženo, že ne všichni lidé mají možnost kryptoměny používat, jelikož se v jejich blízkosti nevyskytuje žádný kamenný obchod. Díky tomu je zřejmé, že ani transakcí nebude tolik jako při běžném každodenním nákupu rohlíků kreditní kartou. Následující grafy znázorňují černými tečkami počet transakcí dané kryptoměny za den a spojnicovou čárou její kurz.

Obr. 4. 5 Vztah mezi kurzem BTC a počtem transakcí (2009–2018)

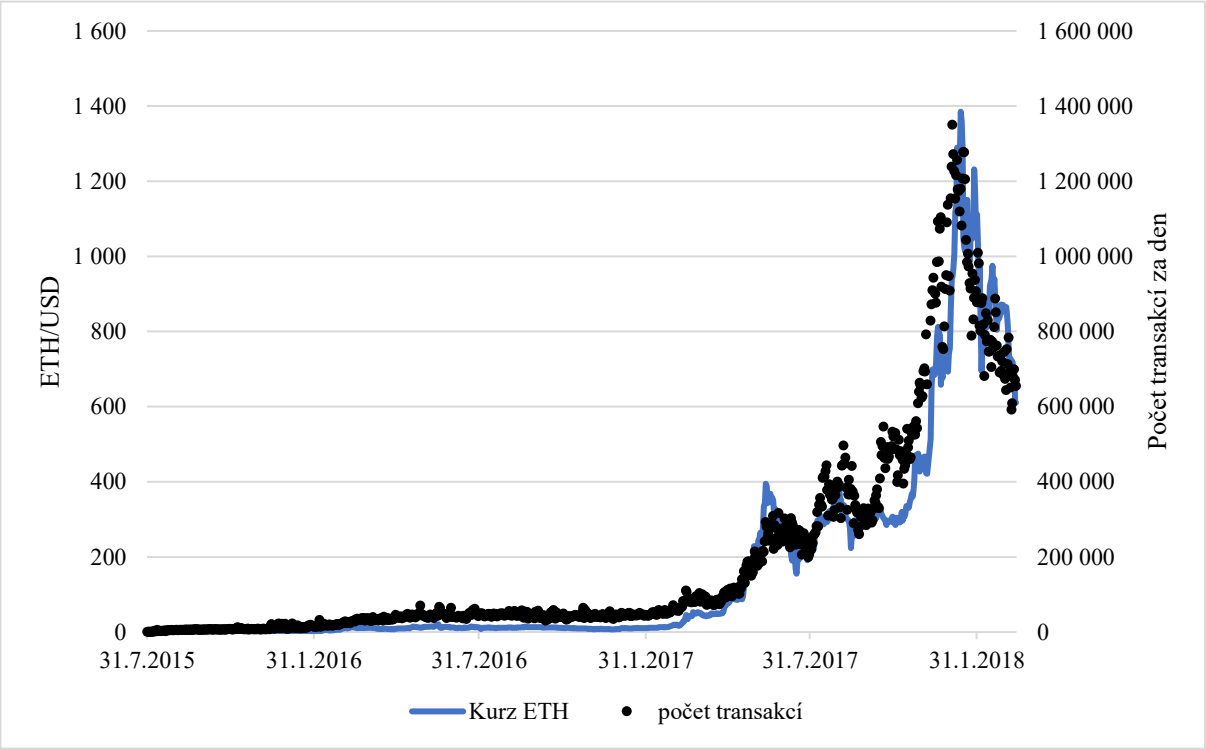


Zdroj: Blockchain (2018), vlastní úprava

Na obrázku 4.5 je znázorněno, jaký je kurz Bitcoinu. Od roku 2017 se drží poměrně vysoko oproti předchozím rokům. Černými tečkami je znázorněno množství transakcí, které proběhlo za každý den. Největší počet transakcí za den byl zaznamenán ke konci roku 2017, kdy byl zároveň i největší kurz Bitcoinu v historii. Pomocí Pearsonova korelačního koeficientu je možné zjistit společný vývoj mezi těmito dvěma proměnnými.

Pearsonův korelační koeficient, kterým je měřena lineární závislost mezi kurzem Bitcoinu a počtem transakcí za den, udává hodnotu rxy= 0,568. Jelikož je tato hodnota vyšší než nula, jde o významnou korelační závislost, která je přímá. Jelikož je hodnota vyšší než 0,5, ale nižší než 0,7, je možné velmi přibližně tvrdit, že se jedná o významnou vazbu mezi oběma veličinami.

Obr. 4. 6 Vztah mezi kurzem ETH a počtem transakcí za den (2015-2018)



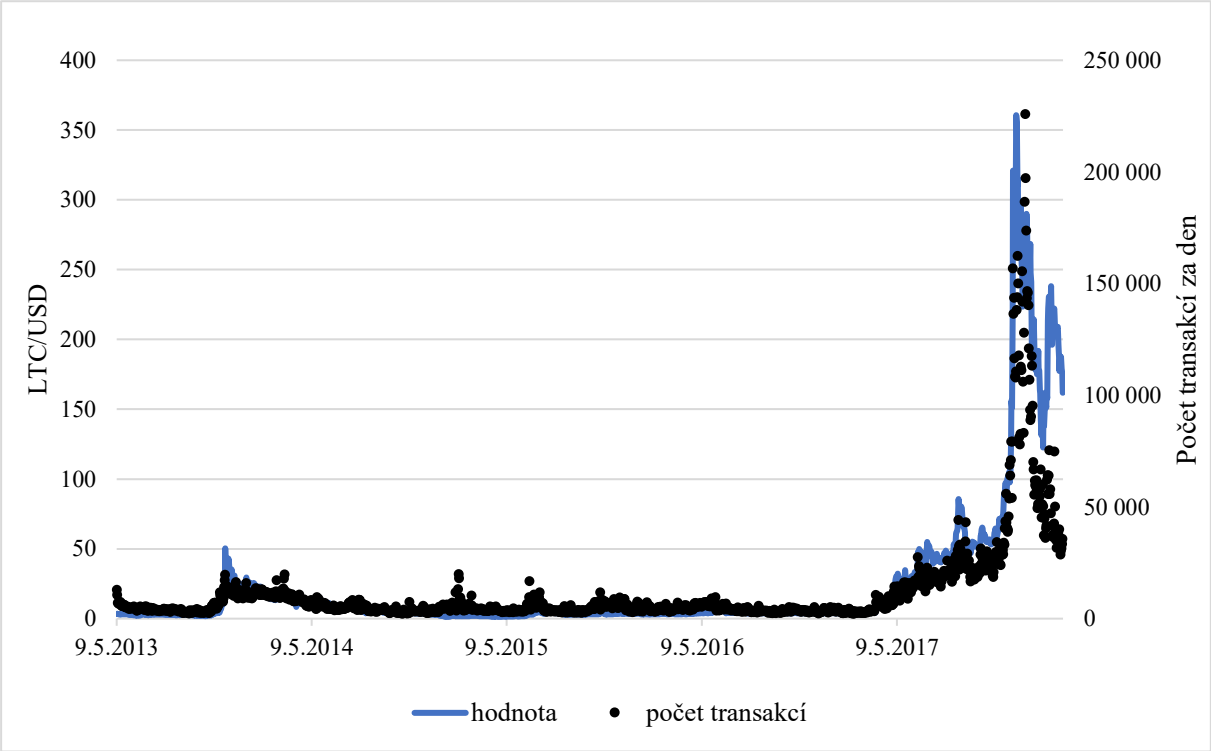
Zdroj: Etherscan (2018), vlastní úprava

Na obrázku 4.6 lze vidět graf, kde spojitá čára opět značí kurz Etherea, který byl stejně jako u Bitcoinu nejvyšší na konci roku 2017. Černé body, které značí počet transakcí za den, se u grafu ve velké míře shlukují v okolí souvislé čáry. Vypočtený Paersonův korelační koeficient mezi kurzem Etherea a trasakcemi, které proběhnou za den, se rovná 0,966. Jelikož je to hodnota kladná a vyskytující se v rozmezí 0,9 až 1, jedná se pravděpodobně o velmi vysokou korelační závislost.

Vztah mezi kurzem Litecoinu a počtem plateb za den, který je možné vidět na obrázku 4.7, je velmi obdobný jako u Etherea. I kurz zároveň s množstvím transakcí byl největší koncem roku 2017. Poté spadl téměř na polovinu. Závislost je opět patrná již z grafu, podle Paersonova koeficientu vykazuje hodnotu 0,915. Podle přibližné stupnice závislosti se jedná opětovně o velmi vysokou závislost mezi proměnnými. Hodnoty proměnných jsou znázorněny až od roku

2013 (téměř dva roky po uvedení Litecoinu do oběhu), kvůli zanedbatelným, téměř nulovým hodnotám.

Obr. 4. 7 Vztah mezi kurzem LTC a počtem transakcí za den (2013-2018)



Zdroj: CryptoID (2018), vlastní úprava

4.1.2 Kryptoměny a zúčtovací jednotka

Dalším znakem tradičních peněz, které jsou používány po celém světě, je zúčtovací jednotka. V podstatě nám tato jednotka udává, za kolik peněz je možné si dané aktivum koupit. Lze ji tedy vyjádřit přesným číslem například v dolarech nebo v českých korunách. Zároveň je tato jednotka dělitelná a díky tomu je možné si nakoupit levná aktiva za malou částku (euro je složeno z centů). I na tento znak dělitelnosti vývojáři kryptoměn mysleli. U Bitcoinu například existuje nejmenší jednotka satoshi, která se rovná 0,000 000 01 BTC, viz kapitola 3.1. Jelikož je nyní možné si za bitcoiny, litecoiny i ethery koupit mnohá aktiva, lze je pokládat za zúčtovací jednotku. Všechno ale záleží na místech, kde a co se dá kryptoměnami zaplatit a také na jejich volatilitě, která je v dnešní době stále vysoká.

Volatilita

Tato podkapitola obsahuje grafy s kurzy Bitecoinu, Litecoinu, Etherea a kromě toho i jeden graf kurzu vybrané fiat měny eura a jeden graf vzácných kovů zlata. Všechny tyto grafy jsou vyjádřeny v dolarech. U každého z nich je spočítán matematickými výpočty rozptyl a variační koeficient daného souboru. Šalounová (2013) uvádí, že jsou souhrnně označovány

jako míry variability. Čím nižší je výsledek ukazatelů variability, tím je větší stejnorodost jednotek vybraného souboru. Naopak čím větší je zkoumaný výsledek, tím více to ukazuje na volatilitu souboru. Prvním ukazatelem je rozptyl. Rozptyl udává, jak moc jsou data rozptýlená kolem aritmetického průměru. Pokud by byl soubor zkoumán jen na základě tohoto aritmetického průměru, neměl by až takovou vypovídací hodnotu kvůli odlehlým hodnotám. Rozptyl naopak dává větší váhu extrémním hodnotám. Ve zjednodušené úpravě pro soubory s větším množstvím dat je vhodné rozptyl (s^2) spočítat takto:

$$s^2 = \frac{\sum_{i=1}^{N} x_i^2 - N\bar{x}^2}{N} = \overline{x^2} - \bar{x}^2, \tag{4.2}$$

kde N udává počet dat, x_i představuje jednotlivá data a $\bar{x}$ jsou průměry dat. Druhým ukazatelem je variační koeficient. Jelikož se všechny následující kurzy výrazně liší aritmetickým průměrem, je vhodné použít tento variační koeficient namísto míry absolutní variability. Výsledkem je bezrozměrná hodnota, která po vynásobení 100 určuje procentní variabilitu. Pokud je výsledek větší než 50 %, je možné přibližně říct, že je daný soubor nesourodý. Variační koeficient (v_x) se spočítá jako:

$$v_x = \frac{s_x}{\bar{x}}, \tag{4.3}$$

Obr. 4. 8 Kurz 1 BTC v USD (2010-2017)

Zdroj: Blockchain (2018), vlastní úprava

kde s_x je směrodatnou odchylkou a $\bar{x}$ je aritmetickým průměrem souboru.

Na obrázku 4.8 lze vidět kurz Bitcoinu vyjádřený v dolarech. V posledním roce 2017 kurz začal prudce stoupat až do přibližné hodnoty 19 289 dolarů za jeden bitcoin, která byla zaznamenána 17.12.2017. Od té doby kurz klesal až na přibližně polovinu své nejvyšší hodnoty. Vypočítaný rozptyl kurzu BTC/USD, do kterého nejsou započítány počáteční nulové hodnoty Bitcoinu, se rovná 6 681 678. Výsledek je příliš vysoký a ukazuje tak na velké rozptýlení dat okolo aritmetického průměru. Tohle tvrzení lze i vidět na grafu, kde se 1 BTC rovnal jak hodnotě 0, tak později i hodnotě až přes 19 000. Dalším výpočtem pomocí koeficientu variace, který se rovná 2,53 (po vynásobení 253 %), je tvrzení o vysoké volatilitě potvrzeno. Tato hodnota udává značnou nesourodost, která vzniká už při hodnotě vyšší než 50 %.

Obr. 4. 9 Kurz 1 ETH v USD (2015-2018)

Zdroj: Etherscan (2018), vlastní úprava

Kurz Etherea, který lze vidět na obrázku 4.9, se přibližně po dobu dvou let držel víceméně na nule. Teprve až od poloviny roku 2017 začaly mít ethery významnou hodnotu a od té doby měl kurz stoupající trend. Stejně jako většina jiných kryptoměn, která převážně reagovala na zamýšlenou regulaci Jižní Korey, tak i cena jednoho etheru v prosinci strmě klesla dolů až na cca polovinu své dosavadní hodnoty. Dosazením dat kurzu do rovnice 4.2 je zjištěn výsledek, který se rovná 76 374,54. Tato hodnota je výrazně menší než u kurzu Bitcoinu, avšak i tak je to hodnota oproti následujícím grafům velmi vysoká. Lze se tedy držet tvrzení, že i Ethereum je vysoce volatilní a jako zúčtovací jednotka není zcela optimální. Do vzorce

byla opět dosazena data bez počátečních nul. Při zjišťování koeficientu variace byla volatilita rovněž potvrzena s výsledkem 173 %. Ve srovnání s Bitcoinem je Ethereum méně volatilní, ale vzhledem k času, za který jsou obě kryptoměny na trhu, není toto tvrzení příliš vypovídající.

Obr. 4. 10 Kurz 1 LTC v USD (2013-2018)

Zdroj: CryptoID (2018), vlastní úprava

Litecoin je na trhu od roku 2011. Ze začátku své existence, jako skoro všechny kryptoměny, měl nulovou hodnotu, a proto je obrázek 4.10 zaznamenaný až od dubna 2013, kdy cena jednoho litecoinu stoupla na vyšší hodnotu. Je zajímavé sledovat, že výrazněji kurz stoupl opět od poloviny roku 2017 a poté začal v prosinci zřejmě z podobných důvodů znovu klesat. Měřený rozptyl dat vychází na 2 620,722. Ukazuje to stále na vysoké rozptýlení, ale ze všech tří kryptoměn je zároveň nejnižší. Je to dané tím, že podle obrázku 4.9 jde vidět, že nejvyšší dosažená hodnota kurzu byla pouze něco málo přes 360 dolarů za jeden litecoin. I tak je ale možné pozorovat vysokou volatilitu. Variační koeficinent, který se v tomto případě dat rovná 222 %, potvrzuje domněnku o velké volatilitě.

Kryptoměny, převážně Bitcoin i Litecoin, jsou často svými vlastnostmi přirovnávány ke zlatu. Hlavním společným znakem je omezené množství. Znamená to, že po vytěžení už nebude možné nalézt žádné nové jednotky ani zlata, ani Bitcoinu. Rovněž bylo zlato kdysi používáno jako platidlo. Mělo ale mnohé nevýhody v podobě špatné dělitelnosti na menší části a nebylo příliš vhodné na přenášení či uchovávání ve velkém množství. Následující obrázek 4.11 tak ukazuje kurz 1 trojské unce zlata vyjádřený v dolarech a zkoumá opět jeho rozptyl

a variaci. Graf znázorňuje kurz přibližně od té doby, kdy byla na trhu uvedena první kryptoměna známá jako Bitcoin. Dále zde nejsou uvedena data z víkendů a svátků. Podle statistických výpočtů se rozptyl okolo aritmetického průměru kurzu rovná 36 575,08. Je tak potvrzeno, že i zlato má velkou škálu hodnot v rozmezí téměř osmi let. Naopak variační koeficient vychází na pouhých 14 % oproti kryptoměnám. Znamená to, že volatilita hodnoty není tak vysoká a nemění se najednou obrovským tempem nahoru nebo dolu, jak je tomu například u Bitcoinu.

Obr. 4. 11 Kurz 1 trojské unce zlata v USD (2010-2018)

Zdroj: Quandl (2018), vlastní úprava

Poslední porovnávanou veličinou je kurz tradiční měny vůči dolaru zobrazený na obrázku 4.12. Tradiční měna neboli fiat měna by patrně měla plnit všechny funkce peněz. Jelikož plní funkci i zúčtovací jednotky, neměla by být výsledná volatilita vysoká. Pro potvrzení očekávání byly použity oba dva vzorce. Výsledný rozptyl kurzu dle rovnice 4.2, který je opět zahrnutý až od doby fungování Bitcoinu, vychází velmi nízký, a to okolo hodnoty 0,013. Jak jde vidět na grafu, tak za dobu osmi let kurz eura stoupal nebo klesal v rozmezí pouhých (1,5-1) 0,5 dolarů za jedno euro. Proto je rozptyl okolo aritmetického průměru kurzu eura tak nízký. Variační koeficient eura k dolaru je 9,2 %. Tato hodnota rovněž vypovídá o nízké variabilitě.

Výsledky potvrdily domněnku o tom, že kryptoměny jsou stále velice volatilní a nejsou tedy příliš vhodné jako zúčtovací jednotky. Člověku se nevyplatí držet velký obnos kryptoměn, když počítá jeden den s tím, že za určitou sumu kryptoměn si koupí auto a další den si za ně sotva může dovolit půlku auta. Je možné, že se jednou hodnota kryptoměn po vytěžení ustálí, ale v současné době o plnění zúčtovací jednotky nelze hovořit v dostatečné míře.

Obr. 4. 12 Kurz 1 EUR v USD (2010-2018)

Zdroj: Quandl (2018), vlastní zpracování

4.1.3 Kryptoměny a uchovatel hodnoty

Poslední funkcí peněz je funkce uchovatele hodnoty. Již podle názvu je zřejmé, že se jedná o cenu peněz, která by se v čase měla uchovat a neměla by příliš ztrácet na své hodnotě. Hodnota kryptoměn je dána především jejich nabídkou a poptávkou. Nabídku určuje omezené množství kryptoměn, jež je popsáno v kapitole 2.2.1. Jediné Ethereum nedisponuje znakem omezeného množství. Poptávku naopak určuje důvěra a počet uživatelů, počet transakcí, investicí, rozvinutost technologii, jednoduchost peněženek pro obyčejné uživatele. Každopádně i tento výrok je podložen grafy o závislosti těchto ukazatelů v kapitole 4.1.1. V následující podkapitole jsou znázorněny tabulky, na kterých je uveden procentní nárůst či pokles hodnoty kurzu kryptoměn vůči dolaru. Poslední dvě tabulky slouží ke srovnání procentního nárůstu či poklesu zlata a tradiční měny, v tomto případě opět eura. Výsledná data jsou opět silně ovlivněna volatilitou dané měny.

Tab. 4. 1 Procentní změny kurzu BTC (2010-2017)

rok	1.1. BTC/USD	31.12. BTC/USD	nárůst/pokles %
2010	0,074	0,299	305
2011	0,299	4,995	1 565
2012	5,499	13,59	147
2013	13,4	739,1	5 416
2014	746,9	317,4	-58
2015	316,15	428	35
2016	432,33	952,156	120
2017	997,729	14 165,575	1 320

Zdroj: Blockchain (2018), vlastní zpracování

V tabulce 4.1 je znázorněno, o kolik procent každý rok stoupl nebo poklesl kurz Bitcoinu vůči dolaru. Pro leden 2010 byla použita první nenulová hodnota z 18.8. Z informací, které jsou patrné z tabulky, je možné vyčíst, že největšího ročního procentního nárůstu dosáhl Bitcoin v roce 2013. Do té doby souvisela cena BTC vesměs s dostupností technologií a jiných komponentů. Od roku 2013 začal být Bitcoin v povědomí obchodníků, závisel na regulacích vlád, na krachu burz či připojení k obchodování. V roce 2014 je možné si všimnout jediného procentního poklesu. Tento pokles je daný mnoha faktory, mezi které se řadí i odhalení černého tržiště Silk Road 2.0, kde probíhaly transakce pomocí BTC. Rok 2017 je klíčovým rokem, kdy širší veřejnost začala mít ponětí o kryptoměnách a mnozí z nich začali s těmito měnami obchodovat. Lze tak z tabulky vyčíst vysoký procentní nárůst, který by byl ještě větší okolo 17. prosince, kdy se hodnota 1 BTC rovnala přibližně 19 829 USD. V tomto případě by se jednalo o 1 833% nárůst.

Další zkoumanou kryptoměnou je Ethereum. Jelikož je na trhu teprve krátce, jsou k dispozici v tabulce 4.2 pouze tři roky dat. V prvním roce, kdy byla použita první nenulová hodnota ze dne 8.7.2010, je celkový pokles -68 %. Od té doby hodnota jednoho etheru v dolarech stoupá vysokou rychlostí. V roce 2017 hodnota stoupla o více jak 9 000 %. Tento nárůst souvisí jak s přibývajícími uživateli, tak s aliancí EEA. EEA (2018) uvádí, že tato aliance sdružuje významné firmy jako Microsoft, ING, Intel a jiné. Společně se snaží vytvořit bezpečný podnikový software, založen na principu smart contractu a blockchainu. Tento software by měl být složitější, náročnější, rychlejší a pomohl by tak mnoha odvětvím, jako je zdravotnictví, podnikání, bankovnictví apod. Ethereum se tak stává významnou kryptoměnou, která má tendenci svým významem předčít i známé kryptoměny jako Bitcoin či Litecoin.

Tab. 4. 2 Procentní změny kurzu ETH (2015-2017)

rok	1.1. ETH/USD	31.12. ETH/USD	nárůst/pokles %
2015	3	0,95	-68
2016	0,92	8,05	775
2017	8,14	741,13	9 005

Zdroj: Etherscan (2018), vlastní úprava

Poslední kryptoměnou, jež je zaznamenána v tabulce 4.3, je Litecoin. V roce 2014 může za procentní pokles hodnoty Litecoinu vůči dolaru hlavně vyjádření jejího tvůrce Charlieho Lee, který prohlásil, že v té době už Litecoin nepotřebuje žádný další vývoj, uvádí Coindesk (2018). Mnoho uživatelů tak kryptoměnu přestalo užívat. Díky tomu poklesla poptávka po kryptoměně i její hodnota. Obrovský procentní nárůst hodnoty Litecoinu lze sledovat v roce 2017. Stejně jak u Bitcoinu, tak i zde za takové obrovské zhodnocení může přístup významných společností na trh kryptoměn, legalizace některých vlád a investice uživatelů, kteří za investicí vidí velké zhodnocení svých peněz. Zároveň je možné tvrdit, že za zvýšení hodnoty LTC může aktivace technologie SegWit, která zlepšuje kapacity transakcí a eliminuje chyby sítě.

Tab. 4. 3 Procentní změny kurzu LTC (2013-2017)

rok	1.1. LTC/USD	31.12. LTC/USD	nárůst/pokles %
2013	4,299	24,446	469
2014	24,591	2,734	-89
2015	2,714	3,475	28
2016	3,512	4,361	24
2017	4,503	237,571	5 176

Zdroj: Quandl (2018), vlastní úprava

Následující tabulka 4.4 obsahuje data o vývoji cen vzácného kovu zlata. Od roku 2010 hodnota kurzu zlata v dolarech rostla i klesala. Jako první datum v roce je vždy použitý termín 2.1., jelikož 1.1. je svátek a hodnota zlata se přes svátek ani přes víkend neudává. Je-li 2.1. víkend, je použit hned následující den. To samé se týká posledního dne v roce. Vychází-li 31.12. nebo i 30.12. na víkend, jsou použity hodnoty ze dne předchozího. Hodnota kurzu zlata má mnoho faktorů, které ovlivňují její kurz. Kurz se mění nalezením nového těžebního místa, tudíž zvýšením nabídky nebo naopak zvýšením poptávky. Například mnoho investorů stále rádo investuje do zlata, jelikož je hmatatelné a jinak řečeno je podloženo samo sebou. Mnoho peněz, hlavně kryptoměn, v dnešní době není podloženo žádným vzácným kovem. Okolo roku 2010

až 2012 kurz zlata stále stoupal, následně do roku 2015 klesal a od té doby začíná opět stoupat. Z tabulky 4.4 si lze všimnout, že oproti tabulkám předchozím nejsou procentní změny tak vysoké. Jednak proto, že není zlato tak moc volatilní a jednak proto, že je to kov starý, je dlouho na trhu, a tudíž není tak lehce ovlivnitelný malými změnami na trhu, jako kryptoměny.

Tab. 4. 4 Procentní změny kurzu zlata (2010-2017)

rok	2.1. AU/USD	31.12. AU/USD	nárůst/pokles %
2010	1 118,9	1 410,25	26
2011	1 405,5	1 574,5	12
2012	1 590	1 664	5
2013	1 681,5	1 201,5	-29
2014	1 219,75	1 199,25	-2
2015	1 184,25	1 062,25	-10
2016	1 072,7	1 159,1	8
2017	1 148,65	1 296,5	13

Zdroj: Quandl (2018), vlastní úprava

Euro je vybrané jako zástupce tradičních měn. Je to běžně používané platidlo, kterým platí 19 zemí Evropské unie. Jeho hodnota vůči dolaru je mimo jiné ovlivněna ekonomickými podmínkami zemí eurozóny. Jelikož jsou všechny hodnoty v tabulce 4.5 vyšší jak 1, znamená to, že je euro silnější měnou vůči dolaru. Následně je z tabulky patrné, že každoročně lze sledovat určitý procentní nárůst nebo pokles hodnoty eura.

Tab. 4. 5 Procentní změny kurzu EUR (2010-2017)

rok	1.1. EUR/USD	31.12. EUR/USD	nárůst/pokles %
2010	1,4389	1,3362	-7
2011	1,3348	1,2939	-3
2012	1,2935	1,3194	2
2013	1,3262	1,3791	4
2014	1,3658	1,2141	-11
2015	1,2043	1,0887	-10
2016	1,0898	1,0541	-3
2017	1,0533	1,1993	14

Zdroj: Quandl (2018), vlastní zpracování

Ze všech pěti sledovaných tabulek jsou změny nejmenší. Díky tomu je možné euro brát jako tradiční měnu, která splňuje roli uchovatele hodnoty. Důvodem jsou nepatrné rozdíly v ceně a žádná velká volatilita měny, která by mohla mít za následek ohrožení hodnoty peněz, které člověk drží.

Na poslední tabulce 4.6 je možné vidět rozdíly mezi kryptoměnami, kovem a tradiční měnou a lze zde porovnat rozdíly výkyvů, nárůstu či poklesů. Je zajímavé sledovanost pokles všech zkoumaných veličin v roce 2014, kdy každá měna vykazovala pokles své hodnoty. V posledním měřeném roce 2017 byl největší nárůst hodnoty zaznamenán u Etherea, (které mělo v roce 2015 největší propad své hodnoty).

Tab. 4. 6 Srovnání procentních změn veličin (2010-2017)

rok	BTC	ETH	LTC	AU	EUR
2010	305	x	x	26	-7
2011	1 565	x	x	12	-3
2012	147	x	x	5	2
2013	5 416	x	469	-29	4
2014	-58	x	-89	-2	-11
2015	35	-68	28	-10	-10
2016	120	775	24	8	-3
2017	1 320	9 005	5 176	13	14

Zdroj: Blockchain (2018), Etherscan (2018), Quandl (2018), vlastní úprava

Závěrem lze říct, že pokud se kryptoměny v budoucnu neustálí na přibližně podobné hodnotě, bude pro ně velmi těžké vyřadit či nahradit fiat měny v každodenním platebním systému. Bitcoin a Litecoin je tak stále v horší pozici oproti Ethereu, které má za hlavní cíl fungování chytrých kontraktů.

4.2 Další faktory ovlivňující budoucnost kryptoměn

Budoucnost kryptoměn ovlivňuje i spousta různých činností lidí. Buď je podporují formou různých technologií nebo se je naopak snaží eliminovat pomocí různých opatření, nařízení, regulací a jiných. V poslední kapitole je tak psáno o těchto důležitých okolnostech, které není možné opomenout.

4.2.1 Zrychlení transakcí LIGTNING NETWORK

Problém u Bitcoinu podle Miškovčík (2018) nastává u rychlosti a poplatků transakce. Tato kryptoměna je schopná za sekundu provést jenom 7 transakcí a poplatky za jednotlivou

transakci v prosinci 2017 dosáhly až 37 $. Oproti tomu například Paypal dokáže provést několik stovek transakcí za sekundu a VISA dokáže odbavit až 24 000 transakcí za sekundu za téměř nulový poplatek. Rozdíl je opravdu markantní, a proto vývojáři přišli s upgradem Lightning Network.

Ligtning Network, jak již bylo zmíněno v kapitole 3.1.3, je aktualizace systému jak u Bitcoinu, tak u Litecoinu, díky které je možné zrychlit transakce a snížit transakční poplatky. Pracuje jako platební kanál Bitcoinu, kde se spojují menší transakce do jedné velké. Podle Cryptosvět (2018) je technologie stále v testovací fázi a cílem vývojářů je opravovat chyby pro dokonalé fungování. Je sice možné používat testovací platební kanály pro uskutečnění reálných transakcí, ale s velkým varováním vývojářů, že díky neopraveným chybám se uživatelům mohou ztratit některé bitcoiny.

Ogurcakova (2018) uvádí, že ačkoliv je technologie pouze v beta verzi, má určitý potenciál stát se reálným platebním kanálem. Tuto technologii podporuje finančně i Charlie Lee, zakladatel Litecoinu, tvůrce Twitteru Jack Dorsey a další. Samotné převody transakcí z malých na jednu velkou provádí síť Ligtning uzlů, která je decentralizovaná. V současnosti má technologie zhruba 2 000 platebních kanálů a 1 000 uzlů.

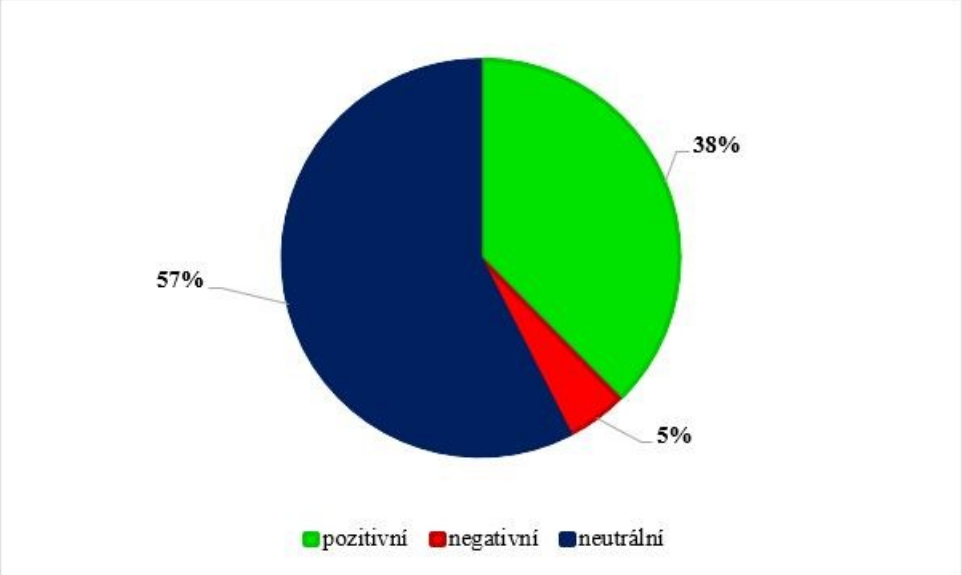
Pro kryptoměny jsou technologie a jejich vylepšování velmi důležité. Díky Lightning Network je možné transakce urychlit a snížit poplatky, a to podporuje roli kryptoměn nahradit platební systém. Pokud bude technologie dovedena k dokonalosti, je možné uvažovat o přibývajících uživatelích.

4.2.2 Regulace vlád

Cena Bitcoinu, Litecoinu, Etherea a samotná důvěryhodnost v kryptoměny se odráží v regulaci jednotlivých států. Kryptomagazín (2018) uvádí, že některé státy považují kryptoměny za nezákonné a jiné je povolují. Velkou regulaci vůči kryptoměnám oznámila vláda v Jižní Koreji, která chce vybírat 22% daň z příjmu právnických osob. A zároveň 2,2% daň z příjmu veškerých burz v zemi, které s kryptoměnami obchodují. Dále vláda nepovolila užívání účtů, jenž jsou anonymní. A to je pro kryptoměny velký zásah, jelikož je to jedna z jejich vlastností. Jižní Korea současně nepovoluje na svých burzách obchodovat uživatelům ze zahraničí. Dalším negativně postaveným státem vůči digitálním měnám je Čína, která má snahu regulovat již od roku 2013. Banky a firmy nesmí obchodovat s kryptoměnami, soukromým subjektům je však obchodování povoleno. Regulace dokonce došly až tak daleko, že vláda zakázala veškeré činnosti kryptoburz. Následující zemí, kde regulace sice ještě

neproběhly, ale v budoucnu určitě proběhnou, je Rusko. USA a Austrálie zamýšlejí v budoucnu veškeré zisky, jenž jsou generovány kryptotrhem, zahrnout do daní. Oproti tomu Švýcarsko je ke kryptoměnám velice pozitivní. V zemi je Bitcoin od všech daní osvobozen a v kantonu Zug je dokonce považován jako prostředek k placení městských poplatků. V České republice zatím platí, že pro obchodování s kryptoměnami není nutné povolení, avšak je nutné oznamovat veškeré transakce, které jsou vyšší než 15 000 €. Celkově mají východní státy oproti západním negativní postavení. Z obrázku 4.12 lze vyčíst, že přibližně 38 % států se staví vůči Bitcoinu pozitivně, respektive nijak neregulují zákony. Dalších cca 5 % států (17 států z celého světa) je postaveno vůči kryptoměně negativně. Mezi tyto státy patří již zmiňovaná Jižní Korea nebo Čína. A zbylých 57 % zemí se stále nevyjádřilo ke svému postoji a zaujímají tak neutrální pozici.

Obr. 4. 13 Postoj států vůči BTC (březen 2018)

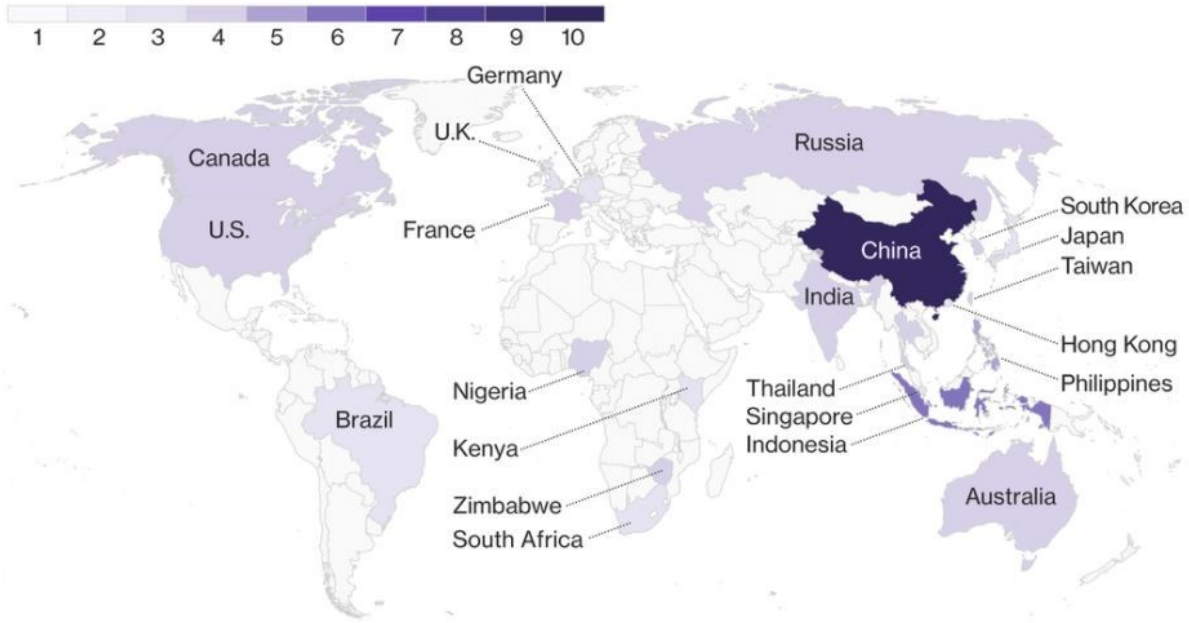


Zdroj: Kryptomagazín (2018), vlastní úprava

Pokud je hlavním cílem Bitcoinu i Litecoinu nahradit platební systém, nejsou regulace příliš vhodné pro další rozvíjení kryptoměny. Vlády pociťují konkurenci vzhledem ke svým fiat penězům, jelikož kryptoměny nejsou nejvhodnější pro výběr daní, kontrolování oběhu peněz ani pro ovládání skrz centrální autoritu. Proto se pomoci regulace snaží eliminovat anonymní účty a snižovat významnost decentralizace kryptoměn. Vlády tak mají vliv na celkovou hodnotu a volatilitu kryptoměn. Tato skutečnost může odradit spoustu lidí. Jelikož zemí, které chtějí provést regulaci, přibývá, je tato skutečnost pro kryptoměny velkou hrozbou pro jejich budoucí nahrazování platebního systému.

Na následujícím obrázku 4.14 je zobrazena mapa světa, kde jsou barevně vybarveny jednotlivé státy podle přístupu k regulaci kryptoměn. Nejtmavší barva ukazuje na státy, které jsou negativně postaveny vůči kryptoměnám. Naopak čím světlejší barvu daný stát má, tím liberálnější postoj zastává. Čína, Jižní Korea i převážná část zemí Oceánie jsou zabarveny tmavou barvou. Díky tomu je jasné, že v těchto zemích existuje spousta zákazů a regulací vůči kryptoměnám. Světlejší barvou jsou vybarveny Spojené státy, Kanada, Rusko, Austrálie, Brazílie a jiné, které zastávají názor, že není třeba kryptoměny zakazovat, ale je nutné je určitým způsobem regulovat. Světle zabarvené státy buď dané kryptoměny vůbec neznají, nebo je pokládají za vhodnou měnou, kterou není třeba nijak měnit či regulovat.

Obr. 4. 14 Mapa regulací kryptoměn ve světě (2018)



Pozn.: 10 = státy s největší regulací kryptoměn, 1= neregulující státy

Zdroj: Bloomberg (2018)

4.2.3 Ostatní události ovlivňující budoucnost kryptoměn

Na budoucnost kryptoměn má vliv spoustá dalších faktorů. Mezi ovlivňitelné faktory se řadí i významné napadení burz. V roce 2014, jak uvádí Fillner (2014) skončila svou činnost burza MtGox. Tato burza byla ve své době největší bitcoinovou burzou. Jelikož se hackerům povedlo z této často nazývané amatérské burzy odcizit 850 tisíc BTC, burza po delší době svou činnost ukončila. Zajímavostí je, že pád této burzy měl na cenu bitcoinu pozitivní vliv, jelikož během pár hodin po uzavření burzy, narostla hodnota o 100 dolarů výše za jeden bitcoin. Tato událost dala velký start pro ostatní burzy, které se snaží o to, aby si získaly důvěru uživatelů. Od té doby proběhly i jiné, menší hackerské útoky na burzy, jako například vykradení

burzy Bitfinex v Hongkongu, kde bylo odcizeno 120 tisíc BTC. I tato suma hodnotou kurzu otřásla. Avšak lze z těchto situací sledovat, že špatné události okolo Bitcoinu jeho dlouhodobou hodnotu naopak posílí.

Bauerle (2018) uvádí, že o budoucnosti kryptoměn i technologie blockchainu nepochybuje. Jelikož se koncem roku 2017 dostaly do širokého povědomí veřejnosti, považují je lidé nyní a unikátní, nezfalšovatelné a nekopírovatelné měny. Samotná technologie blockchain zvládá elektronické bankovnictví, digitální podpisy a je díky ní možné zašifrovat a odšifrovat zprávy, které jsou určené pouze člověku, kterému jsou vyhrazeny. Kryptoměny tak disponují funkcí, kterou fiat měny nemají. S pomocí tohoto faktu jsou kryptoměny zajímavé a mají potenciál stát se novou primární měnou.

5 Závěr

Cílem práce bylo zhodnotit budoucnost Bitcoinu a jiných kryptoměn. Ta se dá hodnotit z hlediska jejich hlavního cíle, který se vyznačuje potenciálem nahradit platební systém.

První část se věnuje penězům, které jsou používány v běžném životě. Historicky fungovaly peníze nejprve jako barterový obchod směnou jednoho zboží za jiné. Následně se používaly komoditní peníze, které představovaly určitý předmět. Nejčastěji to bylo obilí, dobytek či plátno. Nakonec lidé dospěli k tomu, že jejich komoditním zbožím se stanou drahé kovy, jako je zlato, stříbro aj. Tyto kovy splňovaly roli uchovatele hodnoty, a později se začaly razit do malých mincí s podobiznou panovníků. Z těchto mincí se pak postupně přešlo na peníze papírové, které byly lehčí na přenášení. Nakonec se k fyzickým penězům přidaly i peníze uložené na vkladových účtech, díky nimž začalo být jednoduché obchodování napříč světem. Mezi základní funkce peněz patří znaky prostředku směny, zúčtovací jednotky a již zmiňovaný uchovatel hodnoty. Tyto funkce jsou nezbytné pro fungování každodenního oběhu peněz. Následně je v první části práce popsán vznik a zánik peněz, díky kterému jde vidět rozdíl mezi tradičními fiat měnami a kryptoměnami. Tvorba peněz vzniká převážně díky činnosti centrální banky, která může emitovat oběživo. Mnoho odpůrců centralizace peněz uvádí, že stát společně s centrální bankou kradou lidem peníze formou daní a inflací. Těmito odpůrci tak byly vytvořeny kryptoměny, jenž jsou desinflační a které lze těžko danit. Jsou to měny, které jsou anonymní, tudíž se špatně hledá jejich majitel. Dále jsou decentralizační, nejsou tedy téměř ovlivnitelné vládami, mají ve většině případů omezené množství a jejich tzv. účetní kniha je viditelná pro každého uživatele, který si ji chce prohlédnout. Důležité je poznamenat, že první kryptoměny vznikly na popud velké ekonomické krize v roce 2009, kdy na světě vznikalo mnoho odpůrců centralizovaných měn.

Druhá část objasňuje jednotlivé funkce Bitcoinu. Bitcoin údajně vytvořil Satoshi Nakamoto, který je až do dnešní doby anonymní. Během let vznikalo mnoho teorií o bájném tvůrci, ale nikdy nebyly potvrzeny. Bitcoin disponuje peněženkou, ve které je možné si ukládat bitcoiny, ať už jsou v softwarových peněženkách, nebo jsou vytisknuty na papíře jako kombinace číslic a písmen. Transakce probíhají pomocí internetu. Pro potvrzení jednotlivých transakcí uložených do bloku, je nutná činnost těžařů. Ti pomocí hashovacích algoritmů a počítačů hledají správná řešení hash kódu nonce, tzv. prvního řádku určitého bloku. Po vytěžení dostává první úspěšný těžař odměnu 12,5 BTC a transakce obsažené v bloku jsou potvrzeny. Tyto potvrzené transakce je možné najít v blockchainu na internetové stránce, kde si

může jakýkoli uživatel najít, za jakou sumu, kolik a kdy proběhlo transakcí. Blockchain je mimo jiné označován jako účetní kniha. Další zkoumanou kryptoměnou je Ethereum. Ethereum stejně jako Bitcoin je založeno na technologii blockchain, kterou doplňuje o otevřené zdrojové kódy, díky kterým je možné tvořit chytré kontrakty. Blockchain je také používán k nahrazení třetí strany internetu. Neexistuje tak člověk, či skupina lidí, kteří by vlastnili daný server. Všichni uživatelé, používající Ethereum mají možnost servery spravovat. Veškeré změny jsou zaznamenány v blockchainu. Potřebují k tomu akorát tzv. pohon, kterým platí za změny v programu. Tomuto pohonu se říká ethery, což jsou jednotky Etherea. Poslední studovanou kryptoměnou je Litecoin, který se od Bitcoinu liší 4x větším omezeným množstvím a 4x větší rychlostí při potvrzování transakcí. Litecoin je často označován jako mladší bratr Bitcoinu.

V poslední části byla zkoumána empirická část kryptoměn. V první řadě byla srovnána funkce prostředku směny klasických peněz s kryptoměnami. Základním rysem fungování peněz jako prostředku směny je důvěryhodnost. Se stoupající důvěryhodností stoupá rovněž počet uživatelů, kteří kryptoměnu používají jako prostředek směny. Dle zkoumaných grafů bylo zjištěno, že z dlouhodobého hlediska přibývá uživatelů používajících BTC. S důvěryhodností souvisí i počet míst, kde se dá platit bitcoiny. Podle získaných dat lze rozpoznat, že kamenných i internetových obchodů neustále přibývá. Největšího nárůstu obchodů se Bitcoin dočkal v posledních letech. K obchodům se vztahují i bankomaty, kde lze kryptoměny vybrat, nebo vložit. Tyto altcoinové bankomaty mají rovněž narůstající trend, převážně v kontinentech Severní Ameriky a Evropy. Vypovídá to o vřelém vztahu vyspělých zemí k netradičním měnám. Pomocí Pearsonova koeficientu korelace bylo vypočteno, že počet transakcí uživatelů za den má společný průběh s kurzy jednotlivých kryptoměn. Z těchto poznatků vyplývá, že kryptoměny v poměrné výši fungují jako prostředek směny a dostávají se do povědomí stále více lidí. Problémem zůstávají místa ve světě, kde lidé stále nic netuší o těchto alternativních měnách, a tak tyto kryptoměny nyní nemohou zcela nahradit platební systém. Pokud by se obchodníci a jejich obchody rozšířily do všech míst na světě, dalo by se hovořit o možné budoucnosti těchto alternativních měn.

Dále byla zkoumána společná oblast kryptoměn a zúčtovací jednotky. Aby byla splněna tato funkce peněz, muselo by se dát kryptoměnami vyjádřit, kolik jednotek stojí jakékoliv aktivum. Jelikož však ne všechny obchody na světě přijímají tyto měny, tak ani tato podmínka nemůže být stoprocentně splněna. Navíc s vyjádřením ceny jednotlivého aktiva souvisí vysoká volatilita kryptoměn, která je ověřena pomocí rozptylu a koeficientu variace. Všechny zkoumané kryptoměny jsou v čase velice nestabilní oproti tradičním měnám (EUR/USD).

Rozdíl procentuálního vyjádření koeficientu variace jakékoliv kryptoměny a tradiční měny, jenž udává sílu nesourodosti zkoumaných dat, byl více jak dvacetinásobný. Souhrnně lze tvrdit, že pokud se volatilita kryptoměn neustálí a nebude možné pomocí jejich jednotek vyjádřit a zakoupit jakékoliv aktivum, nejsou kryptoměny vhodné pro nahrazení platebního systému.

Další prověřovanou funkcí peněz je uchovatel hodnoty. Tato funkce také souvisí s volatilitou kryptoměn, u kterých není lehké uchovat hodnotu. Pokud by hodnota kurzu těchto měn dlouhodobě klesala nebo by dokonce úplně zanikla, nebyla by splněna úloha uchovatele hodnoty. Názorně byly v kapitole 4.1.3 zobrazeny tabulky ročních procentuálních změn kurzu kryptoměn, zlata i eura k dolaru. Jednotlivé roční změny kurzu u kryptoměn se jeví oproti zlatu a euru vysoké. Kromě roku 2014 a u Etherea roku 2015 jsou procentuální změny v kladných částech. Znamená to, že roční hodnota kurzu neustále stoupá. Neznamená to, že by kryptoměny nyní ztrácely na své hodnotě, nebo by zanikaly. Avšak i takováto vysoká čísla ukazují na vysokou volatilitu kurzu a nemožnosti určit, jestli tato nafouknutá bublina nemůže jednou prasknout. V tomto případě by kryptoměny v krajní nouzi mohly i zaniknout.

Na budoucnost kryptoměn mají rovněž vliv regulace vlád. Regulací v poslední době neustále přibývá. Mezi hlavní odpůrce kryptoměn patří Čína, která nepovoluje bankám ani firmám s kryptoměnami obchodovat. Dále zakazuje činnost kryptoburz, které jsou pro rozšiřování povědomí o těchto měnách velmi důležité. Dalším velkým regulátorem je Jižní Korea, která se původně nezdanitelnou měnu snaží různými způsoby zdanit. Například daní z příjmu právnických osob a jinými. Tyto regulace negativně ovlivňují jak hodnotu kurzu, tak jeho důvěryhodnost, která odrazuje mnoho potenciálních uživatelů. Celkově na světě existuje stále přibližně 38 % států, které zastávají pozitivní postoj, 5 % odpůrců a 57 % neutrálních států, které zatím kryptoměny buď neznají, nebo odmítají vyjádřit svůj postoj.

Závěrem lze říct, že kryptoměny stále čeká dlouhá cesta k tomu, aby byly schopny nahradit současný platební systém. Mezi brzdící faktory patří regulace států, pomalý vývoj technologií, které můžou předčit jiné měny a nutnost mít k dispozici internet. Je nutné, aby se informace o této alternativní měně, která má co nabídnout, dostalo do povědomí široké veřejnosti. Její hlavní klady jsou decentralizace, pseudoanonymita, transparentnost i fakt, že nejsou inflační měnou. Na základě výpočtů je zjištěno, že kryptoměny nesplňují všechny podmínky pro plnohodnotné nahrazení současného platebního systému. Pokud však v budoucnu odstraní jednotlivé již popsané nedostatky, lze tvrdit, že kryptoměny budou mít potenciál stát se primární měnou.

Seznam použité literatury

ACHESON, Noelle, 2016. *How does Proof of Work, um, work?* [online]. DecentralizeToday [28.2.2018]. Dostupné z: https://decentralize.today/how-does-proof-of-work-um-work-f44642b24215

ALZA, 2018. *Ethereum (Vše, co chcete vědět)* [online]. Alza.cz a.s. [5.3.2018]. Dostupné z: https://www.alza.cz/ethereum

BANKY, 2017. *Paypal* [online]. BANKY [1.1.2018]. Dostupné z: https://www.banky.cz/bankovni-slovnik/paypal/

BAUERLE, Nolan, 2017. *What is Blockchain Technology?* [online]. CoinDesk [27.2.2018]. Dostupné z: https://www.coindesk.com/information/what-is-blockchain-technology/

BAUERLE, Nolan, 2018. *CoinDesk's Head of Research On What's Next For Cryptocurrency* [online]. Forbes [27.2.2018]. Dostupné z: https://www.forbes.com/sites/paulinaguditch/2018/02/28/coindesks-head-of-research-on-whats-in-store-for-bitcoin/#3ccc2be6b986

BECKER, Canton, 2017. *Make Paper Wallets to Keep Your Bitcoin Addresses Safe.* [online]. Canton Becker [27.2.2018]. Dostupné z: https://bitcoinpaperwallet.com/

BEŠŤÁK, Ondřej, 2014. *Bitcoin: praktický návod k použití (seriál)* [online]. Mladá fronta [7.2.2018]. Dostupné z: https://www.cnews.cz/bitcoin-prakticky-navod-k-pouziti-serial/

BITCOIN-INFO, 2016. *Jak těžit Bitcoin?* [online]. Bitcoin-info.cz [28.2.2018]. Dostupné z: https://www.bitcoin-info.cz/jak-tezit-bitcoin

BITCOMAP, 2018. *Nákup & prodej v BitcoMATu* [online]. BitcoMAT [25.3.2018]. Dostupné z: https://www.bitcomat.cz/nakup-prodej-v-bitcomatu/

BLOCKCHAIN, 2018. *Bitcoin in circulation* [online]. Blockchain Luxembourg S.A. [5.3.2018]. Dostupné z: https://blockchain.info/charts/total-bitcoins?timespan=all&showDataPoints=true

BLOCKCHAIN, 2018. *Blockchain charts* [online]. Blockchain Luxembourg S. A. [28.3.2018]. Dostupné z: https://blockchain.info/charts

BLOOMBERG, 2018. *Making Sense of the World's Cryptocurrency Rules* [online]. Bloomberg L. P. [25.3.2018]. Dostupné z: https://www.bloomberg.com/crypto

COINATMRADAR, 2018. *Bitcoin ATM map.* [online]. Coin ATM Radar [5.4.2018]. Dostupné z: https://coinatmradar.com/

COINDESK, 2016. *Who is Satoshi Nakamoto?* [online]. CoinDesk [4.1.2018]. Dostupné z: https://www.coindesk.com/information/who-is-satoshi-nakamoto/

COINDESK, 2018. *How Bitcoin Minig Works?* [online]. CoinDesk [28.2.2018]. Dostupné z: https://www.coindesk.com/information/how-bitcoin-mining-works/

COINDESK, 2018. *How do Bitcoin Transaction Work?* [online]. CoinDesk [14.2.2018]. Dostupné z: https://www.coindesk.com/information/how-do-bitcoin-transactions-work/

COINDESK, 2018. *What are Bitcoin Mining Pools?* [online]. CoinDesk [28.2.2018]. Dostupné z: https://www.coindesk.com/information/get-started-mining-pools/

COINDESK, 2018. *What is Bitcoin?* [online]. CoinDesk [5.3.2018]. Dostupné z: https://www.coindesk.com/information/what-is-bitcoin/

COINMAP, 2018. *Coinmap* [online]. CoinMap.org [14.3.2018]. Dostupné z: https://coinmap.org/#/world/49.26780455/16.61132813/4

CRYPTOID, 2018. *Litecoin Blockchain Explorer* [online]. CryptoID.info [20.3.2018]. Dostupné z: https://chainz.cryptoid.info/ltc/#!overview

CRYPTOSVĚT, 2018. *Lightning Network: Co mu brání ve spuštění?* [online]. CryptoSvet.cz [21.3.2018]. Dostupné z: https://cryptosvet.cz/lightning-network-co-mu-brani-v-spusteni/

CSEPCSAR, Kristián 2017. *Úvod do kryptoměn pro vaše tatíky* [online]. Kryptomagazín [1.1.2018]. Dostupné z: https://kryptomagazin.sk/kryptomeny-uvod-pro-tatiky/#_Toc495922364

ČESKÁ NÁRODNÍ BANKA, 2017. *ČNB: Harmonizované peněžní agregáty České republiky* [online]. ČNB [1.1.2018]. Dostupné z: http://www.cnb.cz/cs/statistika/menova_bankovni_stat/stat_mb_met/stat_mb_harmon_agregaty.html

DIGIMĚNY, 2014. *Co je Blochchain?* [online]. Digiměny.cz [27.2.2018]. Dostupné z: http://digimeny.cz/co-je-blockchain/

EEA, 2018. *EEA* [online]. Enterprise Ethereum Alliance [2.4.2018]. Dostupné z: https://entethalliance.org/

ETHEREUM, 2018. *Ethereum: Blockchain App Platform* [online]. Ethereum Foundation [5.3.2018]. Dostupné z: https://www.ethereum.org/

ETHERSCAN, 2018. *Ethereum Transaction Charts* [online]. Etherscan [29.3.2018]. Dostupné z: https://etherscan.io/chart

FAIFE, Corin, 2017. *Bitcoin Hash Functions Explaned* [online]. CoinDesk [27.2.2018]. Dostupné z: https://www.coindesk.com/bitcoin-hash-functions-explained/

FILLNER, Karel, 2014. *Bitcoin Trezor – recenze. Jak mít bitcoiny v bezpečí* [online]. Btctip.cz [7.2.2018]. Dostupné z: http://btctip.cz/bitcoin-trezor-recenze/

FILLNER, Karel, 2014. *MtGox burza končí, bitcoin žije dál* [online]. Btctip.cz [7.2.2018]. Dostupné z: http://btctip.cz/mtgox-burza-konci-bitcoin-zije-dal/

FILLNER, Karel, 2014. *Vlastnosti btc, výhody i nevýhody* [online]. Btctip.cz [7.2.2018]. Dostupné z: http://btctip.cz/vlastnosti-btc-vyhody-i-nevyhody/

HERTIG, Alyssa, 2017. *What is Ethereum?* [online]. CoinDesk [5.3.2018]. Dostupné z: https://www.coindesk.com/information/what-is-ethereum/

INVESTPLUS, 2016. *Těžba kryptoměn: Jak těžit kryptoměny, princip, návratnost, návod na mining* [online]. Investplus [28.2.2018]. Dostupné z: https://investplus.cz/investice/tezba-kryptomen-jak-tezit-kryptomeny-princip-navratnost-navod/

INVESTPLUS, 2017. *Kryptoměny: využití, budoucnost, investiční virtuální měny, diskuze* [online]. Investplus [2.1.2018]. Dostupné z: https://investplus.cz/investice/kryptomeny/

INVESTPLUS, 2018. *Ethereum* [online]. Investplus [5.3.2018]. Dostupné z: https://investplus.cz/kurzy/aktualni-kurz-ethereum-online-graf-kde-koupit-tezba-kryptomeny-cena-hodnota/

INVESTPLUS, 2018. *Litecoin* [online]. Investplus [5.3.2018]. Dostupné z: https://investplus.cz/kurzy/aktualni-kurz-litecoin-online-graf-kde-koupit-tezba-kryptomeny-cena-hodnota/

INVESTPLUS, 2018. *Peněženky pro kryptoměny, kde uchovat virtuální měny, co je TREZOR?* [online]. Investplus [2.1.2018]. Dostupné z: https://investplus.cz/investice/penezenky-pro-kryptomeny-kde-uchovat-virtualni-meny-co-je-trezor/

JÍLEK, Josef, 2004. *Peníze a měnová politika.* Praha: GRADA Publishing, a.s. ISBN 80-247-0769-1.

JÍLEK, Josef, 2013. *Finance v globální ekonomice. I, Peníze a platební styk*. Praha: Grada Publishing. ISBN 978-80-247-3893-2.

JUREČKA, Václav a kol, 2010. *Mikroekonomie.* Praha: GRADA Publishing, a.s. ISBN 978-80-247-3259-6.

KHAOSAN, Venzen, 2014. *How a Bitcoin Transaction Works* [online]. CCN [15.2.2018]. Dostupné z: https://www.ccn.com/bitcoin-transaction-really-works/

KHATWANI, Sudhir, 2018. *What is a Bitcoin Hash?* [online]. CoinSutra [27.2.2018]. Dostupné z: https://coinsutra.com/bitcoin-hash/

KOLLARČÍK, Milan, 2017. *Kdo je Satoshi Nakamoto?* [online]. CryptoSvet [4.1.2018]. Dostupné z: https://cryptosvet.cz/kdo-je-satoshi-nakamoto/

KRYPTOMAGAZIN, 2018. *Bitcoin, kryptoměny, regulace* [online]. Kryptomagazin.cz [20.3.2018]. Dostupné z: https://kryptomagazin.cz/bitcoin-kryptomeny-a-regulace/

MARTUCCI, Brian, 2017. *What Is Cryptocurrency – How It Works, History & Bitcoin Alternatives.* [online]. Money Crashers [6.12.2017]. Dostupné z: https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/

MARTY, 2017. *Vybíráme Bitcoinovou peněženku (praxe II.)* [online]. Bitcoin v Čechách [7.2.2018]. Dostupné z: http://bitcoincz.cz/index.php/2017/02/26/vybirame-bitcoinovou-penezenku-praxe-ii/

MIKSA, Martin 2017. *Bitcoin v mobilu. Kde nakoupit a jaké peněženky používat* [online]. CN Invest a.s. [7.2.2018]. Dostupné z: https://www.mobilmania.cz/bitcoin-v-mobilu-kde-nakoupit-a-jake-aplikace-pouzivat/a-1339897/default.aspx#part=1

MISHKIN, Frederic S, 2013. *The Economics of Money, Banking and Financial Markets.* 10th ed., global ed. Harlow: Pearson. ISBN 978-0-273-76573-8.

MIŠKOVČÍK, Adam, 2018. *Obstojí Bitcoin v boji se svojimi konkurentmi?* [online]. Kryptoportal.sk [21.3.2018]. Dostupné z: https://kryptoportal.sk/obstoji-bitcoin-v-boji-svojimi-konkurentmi/

OGURCAKOVA, Denisa, 2018. *Ligtning Network – instantní převody Bitcoinu jsou o krok blíže k realitě.* [online]. Kryptomagazin.cz [21.3.2018]. Dostupné z: https://kryptomagazin.cz/llightning-networks-instantni-prevody-bitcoinu-jsou-o-krok-blize-k-realite/

QUANDL, 2018. *Data Products* [online]. Quandl Inc. [28.3.2018]. Dostupné z: https://www.quandl.com/search?query=

REVENDA, Zbyněk a kol, 2012. *Peněžní ekonomie a bankovnictví*. 5. aktualiz. vyd. Praha: Management Press. ISBN 978-80-7261-240-6.

REVENDA, Zbyněk, 2013. *Peníze a zlato.* Praha: Management Press. ISBN 978-80-7261-260-4.

ROTHBARD, Murray, 2001. *Peníze v rukou státu: Jak vláda zničila naše peníze.* Praha: Liberální institut. ISBN 80-86389-12-X.

STROUKAL, Dominik a Jan SKALICKÝ, 2015. *Bitcoin: Peníze budoucnosti.* Praha: Ludwig von Mises Institut CZ&SK. ISBN: 978-80-87733-28-8.

ŠALOUNOVÁ, Dana, 2013. *Úvod do pravděpodobnosti a statistiky.* Ostrava: VSB-TU Ostrava 2013. ISBN 978-80-248-3067-4.

TRADEARENA, 2018. *Jak dlouho trvá potvrzení Bitcoinové transakce?* [online]. TRADE – ARENA [15.2.2018]. Dostupné z: https://www.tradearena.cz/rubriky/bitcoin/jak-dlouho-trva-potvrzeni-bitcoinove-transakce_365.html

TRADEARENA, 2018. *Nejlepší Bitcoinová peněženka pro Čechy.* [online]. TRADE-ARENA [7.2.2018]. Dostupné z: https://www.tradearena.cz/rubriky/kryptomeny/nejlepsi-bitcoinova-penezenka-pro-cechy_360.html

Seznam zkratek

AMD	Advanced Micro Devices
ASIC	Application Specific Integrated Circuit
BTC	Bitcoin (jednotka)
CA	Cloud Account
ČNB	Česká národní banka
EEA	Enterprise Ethereum Alliance
EOA	External Owned Account
ETH	Ethereum (jednotka)
EUR	Euro (jednotka)
EVM	Ethereum Virtual Machine
GB	Gigabyte
LTC	Litecoin (jednotka)
P2P	Peer-to-peer
SHA – 256	Secure Hash Algorithm 256
USA	United States of America
USB	Universal Serial Bus
USD	United States Dollar (jednotka)
UTXO	Unspend Transaction Output

Seznam obrázků a tabulek

Prohlášení o využití výsledků bakalářské práce

Prohlašuji, že

- jsem byla seznámena s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, bakalářskou práci užít (§ 35 odst. 3);
- souhlasím s tím, že bakalářská práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že bibliografické údaje o bakalářské práci budou zveřejněny v informačním centru VŠB-TUO
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, bakalářskou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 27.4.2018

Andrea Jezik

jméno a příjmení studenta